J. ALGEBRAIC GEOMETRY
00 (XXXX) 000–000
S 1056-3911(XX)0000-0

IWASAWA THEORY OF THE FINE SELMER GROUP

CHRISTIAN WUTHRICH

Abstract

The fine Selmer group of an elliptic curve E over a number field K is obtained as a subgroup of the usual Selmer group by imposing stronger conditions at places above p. We prove a formula for the Euler-characteristic of the fine Selmer group over a $\mathbb{Z}_p$-extension and use it to compute explicit examples.

1. Introduction

Let E be an elliptic curve defined over a number field K and let p be an odd prime. We choose a finite set of places Σ in K containing all places above $p \cdot \infty$ and such that E has good reduction outside Σ. The Galois group of the maximal extension of K which is unramified outside Σ is denoted by $G_\Sigma(K)$. In everything that follows $\oplus_\Sigma$ always stands for the product over all finite places v in Σ. Let $E\{p\}$ be the $G_\Sigma(K)$-module of all torsion points on E whose order is a power of p. For a finite extension $L : K$, the fine Selmer group is defined to be the kernel

$$0 \longrightarrow \mathcal{R}(E/L) \longrightarrow H^1(G_\Sigma(L), E\{p\}) \longrightarrow \oplus_\Sigma H^1(L_v, E\{p\})$$

where $H^i(L_v, \cdot)$ is a shorthand for the product $\oplus_{w|v} H^i(L_w, \cdot)$ over all places w in L above v. If L is an infinite extension, we define $\mathcal{R}(E/L)$ to be the inductive limit of $\mathcal{R}(E/L')$ for all finite subextensions $L : L' : K$. Note that $\mathcal{R}(E/L)$ does not depend on the choice of the set Σ.

The fine Selmer group has often appeared in the Iwasawa theory of elliptic curves and has different names such as the "strict" or "restricted" Selmer group. We stick to the terminology in [5].

In this article we will be concerned with the behaviour of the fine Selmer group in a given $\mathbb{Z}_p$-extension ${}_\infty K : K$ which will often be the cyclotomic $\mathbb{Z}_p$-extension. Let Γ be the Galois group of ${}_\infty K : K$ and let Λ be the Iwasawa-algebra of Γ. Given a topological generator γ of Γ, we may identify Λ with

Received November 8, 2005.

$\mathbb{Z}_p[\![T]\!]$. It is well known that the Pontryagin-dual of $\mathcal{R}(E/_\infty K)$ is a finitely generated Λ-module.

The same is true of the dual of the classical p-primary Selmer group $\mathcal{S}(E/_\infty K)$. We recall the important results of Perrin-Riou [10] and Schneider [16]. If p is assumed to be an odd prime such that E has good ordinary reduction at all places above p, then there exists a canonical p-adic height pairing on the Selmer group whose regulator is linked to the Iwasawa theory of the Selmer group $\mathcal{S}(E/_\infty K)$. More precisely, if the p-primary part of the Tate-Shafarevich group $Ш(E/K)\{p\}$ is finite and if the regulator does not vanish then the dual of $\mathcal{S}(E/_\infty K)$ is a torsion Λ-module and the order of vanishing of its characteristic power series $f_s \in \Lambda$ at $T = 0$ is equal to the corank of $\mathcal{S}(E/K)$. Moreover the leading coefficient $f_s^*(0)$ of f_s at $T = 0$ can be computed as

$$f_s^*(0) \equiv \mathrm{Reg}_p(E/K) \cdot \frac{\prod_v c_v \cdot N_p^2 \cdot \#Ш(E/K)\{p\}}{(\#E(K)\{p\})^2} \pmod{\mathbb{Z}_p^\times} \tag{1.1}$$

where $\mathrm{Reg}_p(E/K)$ is the normalised p-adic regulator on $E(K)$, N_p is the product of the number of points on the reduction at the places above p and c_v is the Tamagawa number of E at v. Note the importance of the assumption that E has ordinary reduction above p. See for instance [8] for results in the supersingular case.

This article proves the analogous results for the fine Selmer group. One of the important differences is that we are allowed to drop all conditions on the odd prime p. In particular E may have bad reduction of any type and the supersingular situation does not seem to differ in any way from the ordinary situation.

The compact version of the fine Selmer group $\mathfrak{R}(E/K)$ is defined to be the kernel of the following localisation map

$$0 \longrightarrow \mathfrak{R}(E/K) \longrightarrow H^1(G_\Sigma(K), T_pE) \longrightarrow \oplus_{v|p} H^1(K_v, T_pE) \tag{1.2}$$

where $T_pE = \varprojlim E[p^k]$ is the Tate-module of E. It will be shown in Lemma 3.1 that $\mathfrak{R}(E/K)$ is a free $\mathbb{Z}_p$-module whose rank is equal to the corank of $\mathcal{R}(E/K)$.

Perrin-Riou has defined in [11] and [12] a p-adic height pairing on the fine Selmer group $\mathfrak{R}(E/K)$ affiliated with the chosen $\mathbb{Z}_p$-extension. We recall the definition in section 5. Perrin-Riou made the conjecture that the height pairing is non-degenerate. The regulator of the p-adic hieght may be linked to the Iwasawa theory of the fine Selmer group, see Proposition 5.3. It will appear in the formula of the leading term of the characteristic series $f_\mathfrak{X}$ of the dual of the fine Selmer group $\mathfrak{R}(E/_\infty K)$. Other arithmetic invariants of E

also appear, including the order of the fine Tate-Shafarevich group $Ш(E/K)$ with respect to p as defined in [19]. See section 6 for a definition.

We state here the main theorem only in the special situation when the elliptic curve is defined over $\mathbb{Q}$; see Theorem 6.1 for the general statement. If E is an elliptic curve over $\mathbb{Q}$ a much celebrated theorem of Kato [7, Theorem 12.4] states that the dual of $\mathcal{R}(E/_\infty\mathbb{Q})$ is a torsion Λ-module (the so called weak Leopoldt conjecture for E). In the general case this can be checked via the non-degeneracy of the p-adic height on the fine Selmer group. Similarly it is known that the order of vanishing of $f_\mathcal{R}$ at $T = 0$ is equal to the corank of $\mathcal{R}(E/K)$, if the regulator is non-zero; see [11, Proposition 3.4.5] and [12, Corollaire 3.4.3].

Let $_\infty\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let $_n\mathbb{Q}$ be its n^{th} layer.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve whose Tate-Shafarevich group $Ш(E/\mathbb{Q})$ has finite p-primary part. Suppose that the p-adic height on the fine Selmer group is non-degenerate. Then there is an injection with finite cokernel J of $\mathfrak{R}(E/\mathbb{Q})$ into the cokernel of the corestriction map*

$$\mathrm{cor}\colon \varprojlim_n H^1(G_\Sigma({}_n\mathbb{Q}), T_pE) \longrightarrow H^1(G_\Sigma(\mathbb{Q}), T_pE).$$

If the reduction is potentially good, then the leading coefficient of the characteristic power series of the dual of the fine Selmer group $\mathcal{R}(E/_\infty\mathbb{Q})$ is equal to

$$f^*_\mathcal{R}(0) \equiv \mathrm{Reg}(\mathfrak{R}(E/\mathbb{Q})) \cdot \frac{\prod_\upsilon c_\upsilon \cdot \#\,\mathrm{Tors}_{\mathbb{Z}_p}(D) \cdot \#Ш(E/\mathbb{Q})}{\#J} \pmod{\mathbb{Z}_p^\times} \tag{1.3}$$

where D is the cokernel of the localisation map from $E(\mathbb{Q}) \otimes \mathbb{Z}_p$ to the p-adic completion of $E(\mathbb{Q}_p)$.

The proof of the theorem is given in section 7. See Corollary 6.3 for the statement split up according to whether E has rank 0, 1 or greater than 1.

In sections 9, 10 and 11 we include a list of interesting examples. Unlike for the formula 1.1, the expression on the right hand side is not explicitly computable due to the presence of the unknown size of the cokernel J. Nevertheless the formula is still very useful to determine $f_\mathcal{R}$ or even $\mathcal{R}(E/_\infty\mathbb{Q})$. We show how to use the formulae (1.3) and (1.1) and analytic information from [13].

For almost all cases, the result is that $f_\mathcal{R}$ is a simple power of T; in other words that $\mathcal{R}(E/_\infty\mathbb{Q})$ has the same corank as $\mathcal{R}(E/\mathbb{Q})$ and that $Ш(E/_\infty\mathbb{Q})$ is still finite, if $Ш(E/\mathbb{Q})$ is finite. This provides ample evidence that the μ-invariant of the fine Selmer group should always be trivial as conjectured by Coates and Sujatha in [5, Conjecture A].

It is not true that $f_{\mathfrak{R}}$ is always a power of T. The discussion of an example in which the corank of the fine Selmer group over ${}_\infty\mathbb{Q}$ is strictly larger than over $\mathbb{Q}$ is included in section 11. The proof relies on the computation of the rank of the Mordell-Weil over the first two layers of the $\mathbb{Z}_3$-extension.

So far, we cannot find a single example of a curve $E/\mathbb{Q}$ and an odd prime p for which we can prove that the fine Tate-Shafarevich group $Ш(E/{}_\infty\mathbb{Q})$ is infinite. See also Question 8.3 in [19].

Motivated by Proposition 9.2, we make the following

Conjecture 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve. The set of primes p for which the corank of $\mathcal{R}(E/{}_\infty\mathbb{Q})$ is larger than the corank of $\mathcal{R}(E/\mathbb{Q})$ is finite.*

It is a pleasure to thank John Coates, Robert Pollack and Karl Rubin for helpful discussions.

2. Notations

If f is a map between $\mathbb{Z}_p$-modules with finite kernel and cokernel, we write

$$z(f) = \frac{\#\ker(f)}{\#\operatorname{coker}(f)}.$$

For any p-primary abelian group A, the expression A_{div} stands for the maximal divisible subgroup of A and A/div for the quotient of A by A_{div}. The Pontryagin dual of an abelian group A is written $\hat{A}$ and its p-primary part is denoted by $A\{p\}$.

To ease notations of Galois-cohomology we will use the following shorter notations for any $G_\Sigma(K)$-module M :

$$H^i_\Sigma(K,M) = H^i(G_\Sigma(K),M)$$
$$H^i_\Sigma({}_\infty K,M) = H^i(G_\Sigma({}_\infty K),M)$$

The following projective limits along the corestriction maps will often appear

$${}_\infty H^i(E/K) = \varprojlim_n H^i(G_\Sigma({}_n K), T_pE)$$

where T_pE is the Tate module $\varprojlim E[p^k]$. The Γ-module ${}_\infty H^i(E/K)$ does not depend on the choice of the finite set Σ containing all bad places, all places above p and above ∞. It is trivial for $i \neq 1,2$.

If v is a place in K and L is an extension of K, the following notation will be used

$$H^i(L_v,M) = \oplus_{w|v} H^i(L_w,M)$$

whenever M is a module under the absolute Galois group of K_v.

The fine Selmer group $\mathcal{R}(E/K)$ was already defined in the beginning of the introduction. There are also two compact versions of the fine Selmer group; the first is defined by the exact sequence (1.2) and the second smaller group is $\mathfrak{R}_\Sigma(E/K)$, obtained by imposing the local conditions at all places in Σ:

$$0 \longrightarrow \mathfrak{R}_\Sigma(E/K) \longrightarrow H^1_\Sigma(K, T_pE) \longrightarrow \oplus_\Sigma H^1(K_\upsilon, T_pE)$$

It is not difficult to see that $\mathfrak{R}_\Sigma(E/K)$ has finite index in $\mathfrak{R}(E/K)$, since $H^1(K_\upsilon, T_pE)$ is finite if υ does not divide p.

A $\mathbb{Z}_p$-extension ${}_\infty K : K$ can be given as the fixed field of the kernel of a homomorphism $\lambda\colon G_\Sigma(K) \twoheadrightarrow \mathbb{Z}_p$. Conversely a surjective morphism λ in $\mathrm{Hom}(G_\Sigma(K), \mathbb{Z}_p)$ is determined by ${}_\infty K$ up to multiplication by a unit in $\mathbb{Z}_p^\times$. In particular, if σ is an element in $G_\Sigma(K)$, then its action on a basis $\zeta \in T_p\mu$ is given by $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for some $\chi(\sigma)$ in $\mathbb{Z}_p^\times$. Then $\lambda = \frac{1}{p} \cdot \log_p \circ \chi$ defines the cyclotomic $\mathbb{Z}_p$-extension ${}_{\mathrm{cyc}}K$ of K, where $\log_p\colon \mathbb{Z}_p^\times \longrightarrow p\mathbb{Z}_p$ is the p-adic logarithm.

2.1. Global duality. For the proof of the main theorem, the global duality of Poitou-Tate (see [9, Theorem 8.6.8]) will be used. Over the field K, we can extract a five term exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{R}(E/K) & \longrightarrow & H^1_\Sigma(K, E\{p\}) & & \\ & & & & & \searrow & \\ & & & & & & \oplus_\Sigma H^1(K_\upsilon, E\{p\}) \\ & & & & & \swarrow & \\ 0 & \longleftarrow & \mathfrak{R}_\Sigma(E/K)^\wedge & \longleftarrow & H^1_\Sigma(K, T_pE)^\wedge & & \end{array}$$

and a four term exact sequence

$$0 \longrightarrow E(K)\{p\} \longrightarrow \oplus_\Sigma E(K_\upsilon)\{p\} \longrightarrow H^2_\Sigma(K, T_pE)^\wedge \longrightarrow \mathcal{R}(E/K) \longrightarrow 0.$$

Finally, it also shows that $\mathfrak{R}_\Sigma(E/K)$ is dual to the kernel of the localisation map from $H^2_\Sigma(K, E\{p\})$ to $\oplus_\Sigma H^2(K_\upsilon, E\{p\})$. Since the target of this map is trivial by local Tate duality, $\mathfrak{R}_\Sigma(E/K)$ is dual to $H^2_\Sigma(K, E\{p\})$.

The global duality over ${}_\infty K$ can be formulated similarly, e.g. the five term sequence becomes:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{R}(E/{}_\infty K) & \longrightarrow & H^1_\Sigma({}_\infty K, E\{p\}) & & \\ & & & & & \searrow & \\ & & & & & & \oplus_\Sigma H^1({}_\infty K_\upsilon, E\{p\}) \\ & & & & & \swarrow & \\ 0 & \longleftarrow & H^2_\Sigma({}_\infty K, E\{p\}) & \longleftarrow & {}_\infty H^1(E/K)^\wedge & & \end{array}$$

3. The compact fine Selmer group is a free $\mathbb{Z}_p$-module

The snake lemma can be applied to the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)\{p\} & \longrightarrow & H^1_\Sigma(K, T_pE) & \longrightarrow & T_pH^1_\Sigma(K, E\{p\}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \oplus_\Sigma E(K_v)\{p\} & \longrightarrow & \oplus_\Sigma H^1(K_v, T_pE) & \to & \oplus_\Sigma T_pH^1(K_v, E\{p\}) & \to & 0 \end{array}$$

Using that the functor T_p is left-exact, we see that there is an exact sequence

$$0 \longrightarrow \mathfrak{R}_\Sigma(E/K) \longrightarrow T_p\mathcal{R}(E/K) \longrightarrow T_\Sigma$$

where T_Σ is the finite cokernel of the vertical map on the left hand side. The sums in the bottom exact sequence of the previous diagram can be replaced by the sums running only over the places above p, one obtains an injection of $\mathfrak{R}(E/K)$ into $T_p\mathcal{R}(E/K)$ of finite index. Hence we have proved that

Lemma 3.1. *The compact fine Selmer groups $\mathfrak{R}(E/K)$ and $\mathfrak{R}_\Sigma(E/K)$ are free $\mathbb{Z}_p$-modules contained in $T_p\mathcal{R}(E/K)$.*

A counter-example showing that $\mathfrak{R}(E/K)$ is not always equal to $T_p\mathcal{R}(E/K)$ is given in (9) of [19].

In particular the lemma provides us with a map a defined as the dual of the composition

$$\begin{array}{ccc} \mathcal{R}(E/K)^\wedge & \twoheadrightarrow & (\mathcal{R}(E/K)_{\mathrm{div}})^\wedge \\ & & \| \\ & & \mathrm{Hom}_{\mathbb{Z}_p}(T_p\mathcal{R}(E/K), \mathbb{Z}_p) \end{array} \tag{3.1}$$

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_p\mathcal{R}(E/K), \mathbb{Z}_p) \rightarrowtail \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{R}_\Sigma(E/K), \mathbb{Z}_p)$$

Hence a is a map from $\mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{R}_\Sigma(E/K), \mathbb{Z}_p)^\wedge$ to $\mathcal{R}(E/K)$ whose kernel has order

$$\begin{aligned} \#\ker(a) &= [T_p\mathcal{R}(E/K) : \mathfrak{R}_\Sigma(E/K)] \\ &= [T_p\mathcal{R}(E/K) : \mathfrak{R}(E/K)] \cdot [\mathfrak{R}(E/K) : \mathfrak{R}_\Sigma(E/K)] \end{aligned}$$

and the cokernel is dual to $\mathcal{R}(E/K)/\mathrm{div}$. In other words, we have

$$z(a) = \frac{[T_p\mathcal{R}(E/K) : \mathfrak{R}(E/K)] \cdot [\mathfrak{R}(E/K) : \mathfrak{R}_\Sigma(E/K)]}{\#(\mathcal{R}(E/K)/\mathrm{div})}. \tag{3.2}$$

4. Control theorem

We repeat here for the sake of completeness the proof of the well-known control theorem for the fine Selmer group. See for instance Proposition 7.4.4 in [15].

Proposition 4.1. *The restriction map $b\colon \mathcal{R}(E/K) \longrightarrow \mathcal{R}(E/_\infty K)^\Gamma$ has finite kernel and cokernel. The kernel has no more elements than $E(K)\{p\}$ and the cokernel has no more elements than $\prod_{v|p} E(K_v)\{p\} \cdot \prod_{v\nmid p} c_v$, where c_v is the Tamagawa number of E at v.*

Proof. We consider the following commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{R}(E/_\infty K)^\Gamma & \longrightarrow & H^1_\Sigma({}_\infty K, E\{p\})^\Gamma & \longrightarrow & \oplus_\Sigma H^1({}_\infty K_v, E\{p\})^\Gamma \\ & & \uparrow{\scriptstyle b} & & \uparrow & & \uparrow \\ 0 & \longrightarrow & \mathcal{R}(E/K) & \longrightarrow & H^1_\Sigma(K, E\{p\}) & \longrightarrow & \oplus_\Sigma H^1(K_v, E\{p\}) \end{array} \tag{4.1}$$

The Hochschild-Serre spectral sequence yields that the middle vertical map is surjective and its kernel is the group $T_{\mathrm{gl}} = H^1(\Gamma, E({}_\infty K)\{p\})$; similarly the kernel of the vertical map on the right is equal to

$$T_{\mathrm{loc}} = \oplus_\Sigma H^1(\Gamma, H^0({}_\infty K_v, E\{p\})).$$

So there are two exact sequences deduced from the spectral sequence of Hochschild-Serre

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_{\mathrm{gl}} & \longrightarrow & H^1_\Sigma(K, E\{p\}) & \longrightarrow & H^1_\Sigma({}_\infty K, E\{p\})^\Gamma & \longrightarrow & 0 \\ 0 & \longrightarrow & T_{\mathrm{loc}} & \longrightarrow & \oplus_\Sigma H^1(K_v, E\{p\}) & \longrightarrow & \oplus_\Sigma H^1({}_\infty K_v, E\{p\})^\Gamma & \longrightarrow & 0 \end{array} \tag{4.2}$$

The next two lemmata will finish the proof of the proposition. □

Lemma 4.2. *The group T_{gl} is a finite group of order bounded by $E(K)\{p\}$. Moreover, if ${}_\infty K$ is the cyclotomic $\mathbb{Z}_p$-extension and E has potentially good reduction at all primes above p, then T_{gl} has exactly as many elements as $E(K)\{p\}$.*

Proof. Let M be the Γ-module $E({}_\infty K)\{p\}$ and so $T_{\mathrm{gl}} = H^1(\Gamma, M)$. If M is finite, and this is the case under the more restrictive hypothesis of the second statement (see [6]), then $\#H^1(\Gamma, M) = \#H^0(\Gamma, M)$ and so $\#T_{\mathrm{gl}} = \#E(K)\{p\}$. Now let D be the maximal divisible subgroup of M and consider the exact sequence of Γ-modules $0 \longrightarrow T_pD \longrightarrow V_pD \longrightarrow D \longrightarrow 0$, where T_pD is $\varprojlim D[p^k]$ and $V_pD = T_pD \otimes \mathbb{Q}_p$. Since $H^1(\Gamma, V_pD)$ and $H^2(\Gamma, T_pD)$ vanish, we see that D^Γ is finite and $H^1(\Gamma, D)$ is trivial. Now the cohomology of the short exact sequence $0 \longrightarrow D \longrightarrow M \longrightarrow M/D \longrightarrow 0$ shows that $T_{\mathrm{gl}} = H^1(\Gamma, M)$ is equal to $H^1(\Gamma, M/D)$ which has the same number of elements as $H^0(\Gamma, M/D)$. This latter group is equal to the quotient of $M^\Gamma = E(K)\{p\}$ by D^Γ, because $H^1(\Gamma, D)$ vanishes. Hence

$$\#T_{\mathrm{gl}} = \frac{\#E(K)\{p\}}{\#D^\Gamma}.$$

□

Lemma 4.3. *Let v be a finite place of K. The group*

$$T_v = H^1(\Gamma, H^0({}_\infty K_v, E\{p\})$$

is a finite group of order bounded by the order of $E(K_v)\{p\}$. If v does not lie above p, its order is equal to the highest power of p dividing the Tamagawa number c_v. If ${}_\infty K$ is the cyclotomic $\mathbb{Z}_p$-extension, v divides p and the reduction of E at v is potentially good, then the order of T_v is equal to the order of $E(K_v)\{p\}$.

Proof. Let w be any place of ${}_\infty K$ above v. By Shapiro's lemma, T_v is isomorphic to $H^1(\Gamma_w, E({}_\infty K_w)\{p\})$ where Γ_w is the decomposition group of Γ at w. If v splits completely in ${}_\infty K$, then Γ_w is trivial and the statement is clear. Otherwise Γ_w is isomorphic to $\mathbb{Z}_p$ and the proof of the bound can be copied from the proof of the previous lemma.

Finally the statement for the case that v does not lie above p is contained in Lemma 3.4 of [4]. □

5. The height pairing

In this section, we construct the p-adic height pairing on the fine Selmer group. The construction follows closely the original definition of Perrin-Riou in [11], but its presentation is simplified and adapted to our needs. We make a further assumption[1] on the finite set Σ, namely we impose that the class group of the Σ-integers in K is trivial. This can be achieved by adding a set of generators of the class group to the set Σ. The final result in Theorem 6.1 is independent of this choice.

5.1. Extensions. Let $\xi\colon \sigma \longmapsto \xi_\sigma$ be a 1-cocycle representing an element of the compact fine Selmer group $\mathfrak{R}_\Sigma(E/K)$. Its class belongs to $H^1(G_\Sigma(K), T_pE)$, which is equal to $\mathrm{Ext}^1_{G_\Sigma(K)}(T_pE, \mathbb{Z}_p(1))$, i.e. it corresponds to a short exact sequence

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow T_\xi \longrightarrow T_pE \longrightarrow 0 \tag{5.1}$$

of $G_\Sigma(K)$-modules. Explicitly this can be constructed in the following manner: As a $\mathbb{Z}_p$-module T_ξ is just the direct sum $\mathbb{Z}_p(1) \oplus T_pE$, but with the twisted $G_\Sigma(K)$-action given by the the formula

$$(\zeta, Q)^\sigma = (\zeta^\sigma + \langle \xi_\sigma, Q^\sigma \rangle, Q^\sigma) \quad \text{for all } \zeta \in \mathbb{Z}_p(1),\ Q \in T_pE \text{ and } \sigma \in G_\Sigma(K),$$

where we denoted by $\langle \cdot, \cdot \rangle$ the Weil-pairing $T_pE \otimes T_pE \longrightarrow \mathbb{Z}_p(1)$.

[1] This is not strictly necessary but simplifies the exposition.

If v is a place in Σ and G_v any decomposition group at v, then the sequence (5.1) is a split exact sequence of G_v-module. This follows directly from the definition of $\mathfrak{R}_\Sigma(E/K)$, given that $\mathrm{res}_v(\xi)$ is trivial in $H^1(K_v, T_pE)$.

Lemma 5.1. *We have the following diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_\Sigma(K,\mathbb{Z}_p(1)) & \longrightarrow & H^1_\Sigma(K,T_\xi) & \longrightarrow & H^1_\Sigma(K,T_pE) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \oplus_\Sigma H^1(K_v,\mathbb{Z}_p(1)) & \longrightarrow & \oplus_\Sigma H^1(K_v,T_\xi) & \longrightarrow & \oplus_\Sigma H^1(K_v,T_pE) & \longrightarrow & 0 \end{array}$$

Proof. It is already clear why the bottom line is exact. The triviality in the upper left hand corner is due to the fact that $T_pE(K) = 0$. On the right hand side we should complete the diagram with the following square

$$\begin{array}{ccc} H^1_\Sigma(K,T_pE) & \longrightarrow & H^2_\Sigma(K,\mathbb{Z}_p(1)) \\ \downarrow & & \downarrow \\ \oplus_\Sigma H^1(K_v T_pE) & \longrightarrow & \oplus_\Sigma H^2(K_v,\mathbb{Z}_p(1)) \end{array}$$

But we know that the bottom map is trivial and, by global class field theory (see [9, Theorem 8.6.3]), that the map on the right hand side is injective by assumption of the triviality of the class group of the Σ-integers. This proves the lemma. □

We will now apply the snake lemma to the diagram in the previous lemma. The kernel of the vertical map on the right hand side is precisely $\mathfrak{R}_\Sigma(E/K)$. For the left hand side, the global duality of Poitou-Tate, see [9, Theorem 10.3.12], gives an exact sequence

$$H^1_\Sigma(K,\mathbb{Z}_p(1)) \longrightarrow \oplus_\Sigma H^1(K_v,\mathbb{Z}_p(1)) \longrightarrow H^1_\Sigma(K,{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p})^\wedge \longrightarrow 0$$

in which the zero at the end is a consequence of the assumption on the class group of the Σ-integers. The last non-zero term is actually the Galois group $G_\Sigma(K)^{p\text{-ab}}$ of the maximal abelian p-extension of K which is unramified outside Σ. The snake lemma provides us with a map

$$\mathfrak{H}_\xi \colon \mathfrak{R}_\Sigma(E/K) \longrightarrow G_\Sigma(K)^{p\text{-ab}}$$

and hence for every $\mathbb{Z}_p$-extension given by a morphism $\lambda\colon G_\Sigma(K) \twoheadrightarrow \mathbb{Z}_p$ we obtain a pairing

$$\begin{aligned} \langle\cdot,\cdot\rangle_\lambda \colon \mathfrak{R}_\Sigma(E/K)\times\mathfrak{R}_\Sigma(E/K) &\longrightarrow \mathbb{Z}_p \\ (\xi,\eta) &\longmapsto \lambda(\mathfrak{H}_\xi(\eta)) \end{aligned}$$

called the p-adic height pairing affiliated with the $\mathbb{Z}_p$-extension. There is a unique extension of this pairing to the group $\mathfrak{R}(E/K)$:

$$\mathfrak{R}(E/K)\times\mathfrak{R}(E/K) \longrightarrow \mathbb{Q}_p$$

The p-adic regulator of the fine Selmer group $\mathrm{Reg}_\lambda(\mathfrak{R}(E/K))$ is defined to be the determinant of this pairing, which is well-defined up to multiplication by a unit in $\mathbb{Z}_p$. The choice of the surjective morphism λ only changes the regulator by a unit. The pairing is non-degenerate if and only if the regulator is non-zero.

For the rest of the article the following conjecture due to Perrin-Riou, see [11, Conjecture 3.3.7.B.i], will play a crucial role.

Conjecture 5.2. *The p-adic regulator $\mathrm{Reg}_{cyc}(\mathfrak{R}(E/K))$ of the fine Selmer group affiliated with the cyclotomic $\mathbb{Z}_p$-extension is non-zero.*

Starting with the same element ξ, we could also construct an extension

$$0 \longrightarrow {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}(1) \longrightarrow W_\xi \longrightarrow E\{p\} \longrightarrow 0$$

defined as before using the Weil pairing $E\{p\} \otimes E\{p\} \longrightarrow {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}(1)$. Thanks to the assumption on the class group, there is a diagram like before

$$\begin{array}{ccccccc} \longrightarrow & H^1_\Sigma\big(K, {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}(1)\big) & \longrightarrow & H^1_\Sigma(K, W_\xi) & \longrightarrow & H^1_\Sigma(K, E\{p\}) & \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \longrightarrow & \oplus_\Sigma H^1\big(K_v, {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}(1)\big) & \longrightarrow & \oplus_\Sigma H^1(K_v, W_\xi) & \longrightarrow & \oplus_\Sigma H^1(K_v, E\{p\}) & \longrightarrow 0 \end{array}$$

and the snake lemma yields a map

$$\mathcal{H}_\xi \colon \mathcal{R}(E/K) \longrightarrow H^1_\Sigma(K, \mathbb{Z}_p)^\wedge.$$

The $\mathbb{Z}_p$-extension given by $\lambda \in \mathrm{Hom}(G_\Sigma(K), \mathbb{Z}_p) = H^1_\Sigma(K, \mathbb{Z}_p)$ allows us to define a second pairing

$$\begin{aligned} \langle \cdot, \cdot \rangle_\lambda \colon \mathfrak{R}_\Sigma(E/K) \times \mathcal{R}(E/K) &\longrightarrow {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \\ (\xi, \eta) &\longmapsto \mathcal{H}_\xi(\eta)(\lambda) \end{aligned}$$

It is immediate that the dual

$$\hat{a} \colon \mathrm{Hom}(\mathcal{R}(E/K), {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{R}_\Sigma(E/K), \mathbb{Z}_p)$$

of the map a defined in (3.1) sends the second pairing $\mathcal{H}_\xi$ to the first pairing $\mathfrak{H}_\xi$ for all ξ in $\mathfrak{R}_\Sigma(E/K)$.

5.2. Iwasawa theoretic height. The previously defined pairing on the fine Selmer group can be decomposed into a sequence of maps that will link the regulator to the Euler-characteristic of the fine Selmer group.

Fix a topological generator γ of the Galois group Γ of our $\mathbb{Z}_p$-extension given by λ, i.e. $\lambda(\gamma) \in \mathbb{Z}_p^\times$. With this choice, we may identify $H^1(\Gamma, M)$ with the coinvariance M_Γ for all Γ-modules M.

The restriction provides us with a map $b \colon \mathcal{R}(E/K) \longrightarrow \mathcal{R}(E/_\infty K)^\Gamma$ as in Proposition 4.1. The identity induces a map

$$c \colon \mathcal{R}(E/_\infty K)^\Gamma \longrightarrow \mathcal{R}(E/_\infty K)_\Gamma$$

and there is a map

$$d\colon \mathcal{R}(E/_\infty K)_\Gamma \longrightarrow H^1_\Sigma({}_\infty K, E\{p\})_\Gamma$$

coming from the natural inclusion. The spectral sequence of Hochschild-Serre gives a transgression map

$$e\colon H^1_\Sigma({}_\infty K, E\{p\})_\Gamma \rightarrowtail H^2_\Sigma(K, E\{p\}) \tag{5.2}$$

whose cokernel is equal to $H_\Sigma({}_\infty K, E\{p\})^\Gamma$. The global duality in section 2.1 states that there is an isomorphism

$$f\colon H^2_\Sigma(K, E\{p\})^\wedge \xrightarrow{\simeq} \mathfrak{R}_\Sigma(E/K). \tag{5.3}$$

Proposition 5.3. *The p-adic height pairing on the fine Selmer group*

$$h_\lambda\colon \mathfrak{R}_\Sigma(E/K) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{R}_\Sigma(E/K), \mathbb{Z}_p)$$

corresponding to the $\mathbb{Z}_p$-extension λ, given by $h_\lambda(\xi)(\eta) = \langle \xi, \eta\rangle_\lambda$ is equal to the composition in the commutative diagram

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{R}_\Sigma(E/K), \mathbb{Z}_p)^\wedge & & \xrightarrow{\quad\hat{h}_\lambda\quad} & & \mathfrak{R}_\Sigma(E/K)^\wedge \\
\downarrow a & & & & \uparrow f \\
\mathcal{R}(E/K) & & & & H^2_\Sigma(K, E\{p\}) \\
\downarrow b & & & & \uparrow e \\
\mathcal{R}(E/_\infty K)^\Gamma & \xrightarrow{c} & \mathcal{R}(E/_\infty K)_\Gamma & \xrightarrow{d} & H^1_\Sigma({}_\infty K, E\{p\})_\Gamma
\end{array} \tag{5.4}$$

The proof of this proposition is given in section 4.4 of [10] or, in our notations, in [17, I.6].

5.3. The analytic height pairing. In [2] an analytic version of the p-adic height pairing on the fine Selmer group is used to compute some cases of the main conjecture for curves with supersingular reduction. We give here a slightly different formula.

We may suppose the elliptic curve E is given in a Weierstrass equation with integral coefficients. According to Proposition 2 in [18], there exists a subgroup of finite index in $E(K)$, denoted by $E^\bullet(K)$, of points P whose coordinates can be represented as fractions of coprime integers, i.e.

$$P = \left(\frac{a(P)}{e(P)^2}, \frac{b(P)}{e(P)^3}\right)$$

for some elements $a(P)$, $b(P)$ and $e(P)$ in the ring of integers $\mathcal{O}_K$ of K, defined up to multiplication by a unit in $\mathcal{O}_K^\times$.

Proposition 5.4. *Let P and Q be two elements in $\mathfrak{R}(E/K)$ which are in the image of the Kummer map $\kappa\colon E(K)\otimes\mathbb{Z}_p \longrightarrow\!\!\!\!\!\rightarrow H^1_\Sigma(K,T_pE)$. Let $\{P_k\}_k$ and $\{Q_k\}_k$ be sequences of points converging to P and Q in $E(K)\otimes\mathbb{Z}_p$ respectively. Assume that P_k and Q_k belong to $E^\bullet(K)$ for all k. Then the cyclotomic p-adic height pairing of P and Q is equal to*

$$\langle P,Q\rangle_{cyc} = \frac{1}{2p}\cdot\lim_{k\to\infty}\log_p\circ N_{K:\mathbb{Q}}\left(\frac{a(P_k)\cdot a(Q_k)}{a(P_k+Q_k)}\right)$$

where log_p denotes the p-adic logarithm.

For a proof of this formula we refer the reader to [17, Theorem IV.8]. If the p-primary part of the Tate-Shafarevich group $Ш(E/K)$ is finite, then there is a subgroup of finite index in $\mathfrak{R}(E/K)$ for which the above formula applies and hence one could use this formula for computing the p-adic regulator. Nevertheless there is a faster algorithm for its computation using the σ-function of Bernardi [1] and the p-adic elliptic logarithm. For details see section VI.1.1 in [17].

Note also that this formula proves the fact that the pairing is indeed bilinear and symmetric.

6. The Euler-characteristic

Using the choice of a topological generator γ of Γ, we identify Λ with $\mathbb{Z}_p[\![T]\!]$ by sending $\gamma-1$ to T. A torsion Λ-module X gives rise to a characteristic power series f_X which is a non-zero element of Λ, defined up to a unit in $\Lambda^\times$. The leading coefficient of f_X at $T=0$,

$$f_X^*(0) = \left.\frac{f_X(T)}{T^{\mathrm{ord}_T(f_X)}}\right|_{T=0} \in \mathbb{Z}_p\setminus\{0\}$$

is called the Euler-characteristic of the Λ-module X. Its valuation is independent of the choice of γ.

Theorem 6.1. *Let E be an elliptic curve defined over a number field K. Suppose the p-adic height affiliated with a $\mathbb{Z}_p$-extension ${}_\infty K : K$ is non-degenerate. Then*

1. *The dual of $\mathcal{R}(E/{}_\infty K)$ is a torsion Λ-module.*
2. *Let r be the corank of $\mathcal{R}(E/K)$. Then the characteristic power series $f_{\mathcal{R}}(T)$ of the dual of $\mathcal{R}(E/{}_\infty K)$ has a zero of order r at $T=0$.*
3. *There is an injection*

$$\mathfrak{R}(E/K) \rightarrowtail\!\!\!\!\!\succ {}_\infty H^2(E/K)^\Gamma = \left(\varprojlim H^2_\Sigma({}_n K,T_pE)\right)^\Gamma$$

whose cokernel J is finite.

(4) *The leading coefficient of $f_{\mathfrak{R}}$ has the same valuation as*

$$f^*_{\mathfrak{R}}(0) \equiv \mathrm{Reg}_\lambda(\mathfrak{R}(E/K)) \cdot \frac{\#T_{loc} \cdot \#\big(\mathcal{R}(E/K)/\,\mathrm{div}\big)}{\#T_{gl} \cdot \#J \cdot \#I} \pmod{\mathbb{Z}_p^\times}$$

where I is the index of $\mathfrak{R}(E/K)$ in $T_p\mathcal{R}(E/K)$ defined in section 3 and T_{gl} and T_{loc} were defined in (4.2).

The formula can be simplified substantially if one assume more restrictive hypotheses. The following corollaries specify the theorem to cases when the $\mathbb{Z}_p$-extension is cyclotomic. The first three conclusions of the theorem are still valid and so only a reformulation of the leading coefficient of $f_{\mathfrak{R}}$ is given. But first, we need some more definitions: the subgroup of elements in $\mathcal{R}(E/K)$ that belong to the image of the Kummer map $E(K)\otimes^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \longrightarrow H^1_\Sigma(K, E\{p\})$ will be denoted by $\mathcal{M}(E/K)$. The fine Tate-Shafarevich group $\text{Ш}(E/K)$ is defined to be the quotient of $\mathcal{R}(E/K)$ by $\mathcal{M}(E/K)$. It naturally identifies with a subgroup of the p-primary part of the Tate-Shafarevich group $Ш(E/K)$. For properties of this group we refer the reader to [19].

Corollary 6.2. *Assume that E has potentially good reduction at all place above p and that the fine Tate-Shafarevich group $\text{Ш}(E/K)$ is finite. If the cyclotomic p-adic height is non-degenerate then the leading coefficient of the characteristic power series $f_{\mathfrak{R}}$ of the dual of the fine Selmer group $\mathcal{R}(E/_\infty K)$ is equal to*

$$f^*_{\mathfrak{R}}(0) \equiv \mathrm{Reg}_{cyc}(\mathfrak{R}(E/K)) \cdot \frac{\#\,\mathrm{Tors}_{\mathbb{Z}_p}(D) \cdot \prod_{v\nmid p} c_v \cdot \#\text{Ш}(E/K)}{\#J} \pmod{\mathbb{Z}_p^\times}$$

with D being the cokernel of the localisation map from $E(K)\otimes\mathbb{Z}_p$ to the p-adic completion of $\oplus_{v|p}E(K_v)$.

Proof. By Lemma 4.2 we know that T_{gl} has the same order as $E(K)\{p\}$ and Lemma 4.3 tells us that

$$\#T_{\mathrm{loc}} = \prod_{v\nmid p} c_v^{(p)} \cdot \prod_{v|p} \#E(K_v)\{p\} \equiv \prod_{v\nmid p} c_v \cdot \prod_{v|p} \#E(K_v)\{p\} \pmod{\mathbb{Z}_p^\times}$$

under our assumptions. Here $c_v^{(p)}$ is the highest power of p dividing c_v. If the fine Tate-Shafarevich group is finite, then $\mathfrak{R}(E/K)$ coincides with its subgroup $\mathfrak{M}(E/K)$ defined to be the elements in the image of the Kummer map $E(K)\otimes\mathbb{Z}_p \longrightarrow H^1_\Sigma(K, T_pE)$. Similarly $T_p\mathcal{R}(E/K)$ can be replaced by $T_p\mathcal{M}(E/K)$. Now the Theorem 7.1 in [19] can be used to compute I: it states that there is an exact sequence

$$0 \longrightarrow I \longrightarrow T \longrightarrow \mathrm{Tors}_{\mathbb{Z}_p}(D) \longrightarrow \mathcal{M}(E/K)/\,\mathrm{div} \longrightarrow 0 \tag{6.1}$$

with T beings the quotient of $\oplus_{v|p} E(K_v)\{p\}$ by the global torsion points. By the finiteness of $Ш(E/K)$ we have a short exact sequence

$$0 \longrightarrow \mathcal{M}(E/K)/\operatorname{div} \longrightarrow \mathcal{R}(E/K)/\operatorname{div} \longrightarrow Ш(E/K) \longrightarrow 0 \tag{6.2}$$

and hence we can compute modulo $\mathbb{Z}_p^\times$

$$\begin{aligned}\frac{\#T_{\mathrm{loc}}}{\#T_{\mathrm{gl}}} \cdot \frac{\#(\mathcal{R}(E/K)/\operatorname{div})}{\#I} &\equiv \prod_{v\nmid p} c_v \cdot \#T \cdot \frac{\#(\mathcal{M}(E/K)/\operatorname{div}) \cdot \#Ш(E/K)}{\#I} \\ &\equiv \prod_{v\nmid p} c_v \cdot \#I \cdot \#\operatorname{Tors}_{\mathbb{Z}_p}(D) \cdot \frac{\#Ш(E/K)}{\#I}\end{aligned}$$

which finished the proof of the corollary. □

Finally we specify to the case of a curve over $\mathbb{Q}$ and treat the cases of rank 0, 1 and strictly bigger than 1 separately.

Corollary 6.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ with potentially good reduction at p whose Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is finite. The fine Selmer group $\mathfrak{R}(E/\mathbb{Q})$ is trivial if the rank of $E(\mathbb{Q})$ is less than 2 and its rank is equal to $\operatorname{rank}(E(\mathbb{Q}))-1$ otherwise. If $E(\mathbb{Q})$ is finite then*

$$f_{\mathfrak{R}}(0) \equiv \frac{\#E(\mathbb{Q}_p)\{p\} \cdot \prod c_v \cdot \#Ш(E/\mathbb{Q})}{\#E(\mathbb{Q})\{p\} \cdot \#J} \pmod{\mathbb{Z}_p^\times}.$$

If the rank of $E(\mathbb{Q})$ is equal to 1 then

$$f_{\mathfrak{R}}(0) \equiv \frac{\#D \cdot \prod c_v \cdot \#Ш(E/\mathbb{Q})\{p\}}{\#J} \pmod{\mathbb{Z}_p^\times}.$$

If $E(\mathbb{Q})$ has rank strictly larger than 1 and the p-adic height is non-degenerate on the fine Selmer group then

$$f^*_{\mathfrak{R}}(0) \equiv \operatorname{Reg}_{cyc}(\mathfrak{R}(E/\mathbb{Q})) \cdot \frac{\#D \cdot \prod c_v \cdot \#Ш(E/\mathbb{Q})\{p\}}{\#J} \pmod{\mathbb{Z}_p^\times}.$$

Proof. These formulae are simply obtained by specifying the formula in the previous corollary. If the rank of $E(\mathbb{Q})$ is smaller than 2, then $\mathfrak{R}(E/\mathbb{Q})$ is trivial and hence the p-adic height pairing is automatically non-degenerate of regulator equal to 1. If the rank is zero then D is the quotient of $E(\mathbb{Q}_p)$ by $E(\mathbb{Q})\{p\}$. If the rank is positive, then D has to be torsion and by Theorem 3.5 in [19] the fine Tate-Shafarevich group $Ш(E/\mathbb{Q})$ coincides with the p-primary part of $Ш(E/\mathbb{Q})$. Finally the assumption that the reduction is potentially good and that $p \neq 2$ assures that c_p is not divisible by p and the term $\prod_{v\nmid p} c_v$ has the same valuation as the product of all Tamagawa numbers. □

7. Proof of Theorem 6.1

The first two assertions are well-known. The first conclusion, that the dual Y of the fine Selmer group $\mathcal{R}(E/_\infty K)$ is Λ-torsion is usually called the weak Leopoldt conjecture; it is equivalent to the vanishing of $H^2_\Sigma({}_\infty K, E\{p\})$ (see Proposition 1.3.2 in [12]). The two conclusions are now contained in Corollaire 3.4.3 of [12]. A different proof is presented in I.7 and I.8 of [17].

In particular, we deduce that the map e in (5.2) whose cokernel is equal to $H^2_\Sigma({}_\infty K, E\{p\})^\Gamma$ must be an isomorphism. By Proposition 4.1, the map b has finite kernel and cokernel, by (3.2) and (5.3) the same is true for a and f. Since h_λ has the same property by the assumption on the non-degeneracy of the height, all maps in the diagram (5.4), have finite kernel and cokernel except maybe c and d. It follows that the kernel of c is finite. Hence the map $\hat{c}\colon Y^\Gamma \longrightarrow Y_\Gamma$ has finite cokernel and this, together with the fact that Y is Λ-torsion, is sufficient to show that $\hat{c}$ has also finite kernel and that the leading coefficient of $f_\mathfrak{X}$ has the same valuation as $z(c)$. In fact it can be deduced from the decomposition theorem for finitely generated Λ-modules. (See Lemma I.28 in [17] or Lemme 0.2.3 in [10]). It follows now that d has finite kernel and cokernel, too.

Note that the target of d is isomorphic (via e and f) to $\mathfrak{R}_\Sigma(E/K)^\wedge$ which is known to be a divisible group by Lemma 3.1. Hence the finite cokernel of d is trivial. We need the following

Lemma 7.1. *There is a surjective map*

$$\oplus_\Sigma H^1({}_\infty K_\upsilon, E\{p\})^\Gamma \xrightarrow{g} ({}_\infty H^1(E/K)^\wedge)^\Gamma.$$

Proof. Define the group ${}_\infty C$ by the exact sequence

$$0 \longrightarrow \mathcal{R}(E/_\infty K) \longrightarrow H^1_\Sigma({}_\infty K, E\{p\}) \longrightarrow {}_\infty C \longrightarrow 0 \tag{7.1}$$

The global duality in section 2.1 over ${}_\infty K$ allows us to complete this by another exact sequence

$$0 \longrightarrow {}_\infty C \longrightarrow \oplus_\Sigma H^1({}_\infty K_\upsilon, E\{p\}) \longrightarrow {}_\infty H^1(E/K)^\wedge \longrightarrow 0 \tag{7.2}$$

where the last zero comes from the proven weak Leopoldt conjecture, because $H^2_\Sigma({}_\infty K, E\{p\})$ is trivial. So from (7.1) we conclude that

$$\begin{aligned} &0 \longrightarrow \mathcal{R}(E/_\infty K)^\Gamma \longrightarrow H^1_\Sigma({}_\infty K, E\{p\})^\Gamma \longrightarrow {}_\infty C^\Gamma \longrightarrow \\ &\longrightarrow \mathcal{R}(E/_\infty K)_\Gamma \xrightarrow{d} H^1_\Sigma({}_\infty K, E\{p\})_\Gamma \longrightarrow {}_\infty C_\Gamma \longrightarrow 0 \end{aligned} \tag{7.3}$$

is an exact sequence in which the surjective map d appears. Hence ${}_\infty C_\Gamma$ is trivial. From (7.2) we see that

$$0 \longrightarrow {}_\infty C^\Gamma \longrightarrow \oplus_\Sigma H^1({}_\infty K_\upsilon, E\{p\})^\Gamma \longrightarrow \left({}_\infty H^1(E/K)^\wedge\right)^\Gamma \longrightarrow 0 \tag{7.4}$$

and the lemma follows. □

We will need the short exact sequence

$$0 \longrightarrow {}_\infty H^1(E/K)_\Gamma \xrightarrow{\text{cor}} H^1_\Sigma(K, T_pE) \longrightarrow {}_\infty H^2(E/K)^\Gamma \longrightarrow 0 \tag{7.5}$$

which is a consequence of the spectral sequence of Tate, see Theorem II.1.11 and II.1.12 in [9]. The dual of this sequence can now be put together with the two exact sequences (4.2) in a larger commutative diagram:

$$\begin{array}{ccccc}
0 & & 0 & & 0 \\
\uparrow & & \uparrow & & \uparrow \\
H^1_\Sigma({}_\infty K, E\{p\})^\Gamma & \circ\!\!\rightarrow & \oplus_\Sigma H^1({}_\infty K_v, E\{p\})^\Gamma & \circ\!\!\rightarrow & ({}_\infty H^1(E/K)_\Gamma)^\wedge \\
\uparrow & & \uparrow & & \uparrow \\
H^1_\Sigma(K, E\{p\}) & \circ\!\!\rightarrow & \oplus_\Sigma H^1(K_v, E\{p\}) & \circ\!\!\rightarrow & H^1_\Sigma(K, T_pE)^\wedge \\
\uparrow & & \uparrow & & \uparrow \\
T_{\mathrm{gl}} & \circ\!\!\rightarrow & T_{\mathrm{loc}} & \circ\!\!\rightarrow & ({}_\infty H^2(E/K)^\Gamma)^\wedge \\
\uparrow & & \uparrow & & \uparrow \\
0 & & 0 & & 0
\end{array}$$

Here the vertical lines are exact sequences; the horizontal lines are not exact but they form at least a cochain complex (completed with zeros to the left and the right), which is symbolised with the arrows of the form $\circ\!\!\rightarrow$. Note that the top line is the Γ-invariance of a part of the global duality over ${}_\infty K$ as we used it before for the definition on ${}_\infty C$. In order to recover the bottom complex, we take the second sequence exposed in 2.1

$$0 \longrightarrow E({}_\infty K)\{p\} \longrightarrow {}_\infty T \longrightarrow {}_\infty H^2(E/K)^\wedge \longrightarrow \mathcal{R}(E/{}_\infty K) \longrightarrow 0 \tag{7.6}$$

where ${}_\infty T$ is $\oplus_\Sigma H^0({}_\infty K_v, E\{p\})$. The Γ-coinvariance of this sequence gives the desired complex

$$0 \longrightarrow T_{\mathrm{gl}} \circ\!\!\rightarrow T_{\mathrm{loc}} \circ\!\!\rightarrow ({}_\infty H^2(E/K)^\Gamma)^\wedge \longrightarrow \mathcal{R}(E/{}_\infty K)_\Gamma \longrightarrow 0. \tag{7.7}$$

The middle complex of the above huge diagram is actually simply a part of the global duality sequence over K and, hence, is exact in the middle. The long exact sequence associated to this short exact sequence of cochain complexes breaks up into two exact sequences with four terms. Denote the cochain complexes by $Z^\bullet_{\mathrm{top}}$, $Z^\bullet_{\mathrm{mi}}$ and $Z^\bullet_{\mathrm{bo}}$ respectively and fix notations so that their zero-th term is on the middle vertical line. Comparing with (4.1), we

get that the first part is simply

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^{-1}(Z^\bullet_{\mathrm{bo}}) & \longrightarrow & H^{-1}(Z^\bullet_{\mathrm{mi}}) & \longrightarrow & H^{-1}(Z^\bullet_{\mathrm{top}}) & \longrightarrow & H^0(Z^\bullet_{\mathrm{bo}}) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \ker(b) & \longrightarrow & \mathcal{R}(E/K) & \xrightarrow{b} & \mathcal{R}(E/_\infty K)^\Gamma & \longrightarrow & \mathrm{coker}(b) & \longrightarrow & 0 \end{array} \tag{7.8}$$

Lemma 7.1 shows that $H^1(Z^\bullet_{\mathrm{top}}) = 0$. The sequence (7.4) proves that ${}_\infty C^\Gamma$ is the kernel of $Z^0_{\mathrm{top}} \longrightarrow Z^1_{\mathrm{top}}$; together with (7.3) this yields $H^0(Z^\bullet_{\mathrm{top}}) = \ker d$. Finally the sequence (7.7) shows that $H^1(Z^\bullet_{\mathrm{bo}})$ is equal to $\mathcal{R}(E/_\infty K)_\Gamma$, hence we have

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^0(Z^\bullet_{\mathrm{top}}) & \longrightarrow & H^1(Z^\bullet_{\mathrm{bo}}) & \longrightarrow & H^1(Z^\bullet_{\mathrm{mi}}) & \longrightarrow & H^1(Z^\bullet_{\mathrm{top}}) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \ker(d) & \longrightarrow & \mathcal{R}(E/_\infty K)_\Gamma & \twoheadrightarrow & \mathfrak{R}_\Sigma(E/K)^\wedge & \longrightarrow & 0 & & \end{array}$$

We shall prove now the third statement of Theorem 6.1. Since $\ker(d)$ is finite, the previous exact sequence shows that there is an injection of $\mathfrak{R}_\Sigma(E/K)$ into the dual of $\mathcal{R}(E/_\infty K)_\Gamma$ with finite cokernel. (It is actually not difficult to show that this map is the composition $\hat{d}\circ\hat{e}\circ\hat{f}$.) Then from the sequence (7.7), one deduces an injection of the dual of $\mathcal{R}(E/_\infty K)_\Gamma$ into ${}_\infty H^2(E/K)^\Gamma$ whose cokernel lies in the finite group T_{loc}, see Lemma 4.3. Thus we have an injection of $\mathfrak{R}_\Sigma(E/K)$ into the group ${}_\infty H^2(E/K)^\Gamma$ with image of finite index.

There is also a map from $\mathfrak{R}(E/K)$ into ${}_\infty H^2(E/K)^\Gamma$ obtained by sending $\mathfrak{R}(E/K)$ into $H^1_\Sigma(K, T_pE)$, followed by the second map in the sequence (7.5) coming from Tate's spectral sequence. This map restricts to the previous injection on $\mathfrak{R}_\Sigma(E/K)$. Since $\mathfrak{R}(E/K)$ is $\mathbb{Z}_p$-free by Lemma 3.1, the kernel of $\mathfrak{R}(E/K) \longrightarrow {}_\infty H^2(E/K)^\Gamma$ must be trivial.

Finally, we come to the last part of the theorem, namely the computation of $f^*_{\mathfrak{R}}(0) = z(c)$. From the previous computations, we may compute the order of J as

$$\begin{aligned} \#J \cdot [\mathfrak{R}(E/K) : \mathfrak{R}_\Sigma(E/K)] &= [{}_\infty H^2(E/K)^\Gamma : \mathfrak{R}_\Sigma(E/K)] \\ &= \#\ker(d) \cdot [({}_\infty H^2(E/K)_\Gamma)^\wedge : \mathcal{R}(E/_\infty K)^\Gamma] \\ &= \#\ker(d) \cdot \frac{\#T_{\mathrm{loc}} \cdot \#H^1(Z^\bullet_{\mathrm{bo}})}{\#T_{\mathrm{gl}} \cdot \#H^0(Z^\bullet_{\mathrm{bo}})}. \end{aligned}$$

In the last line, we have used the complex (7.7). The identification in (7.8) allows us to rewrite the expression as

$$\begin{aligned} \#J \cdot [\mathfrak{R}(E/K) : \mathfrak{R}_\Sigma(E/K)] &= \#\ker(d) \cdot \frac{\#T_{\mathrm{loc}} \cdot \#\ker(b)}{\#T_{\mathrm{gl}} \cdot \#\operatorname{coker}(b)} \\ &= z(d) \cdot z(b) \cdot \frac{\#T_{\mathrm{loc}}}{\#T_{\mathrm{gl}}} \end{aligned} \tag{7.9}$$

We now compute $z(c)$ using the decomposition of the p-adic height in (5.4), (7.9), (3.2) and the fact that e and f are isomorphisms.

$$\begin{aligned} z(c) &= \frac{z(\hat{h})}{z(f) \cdot z(e) \cdot z(d) \cdot z(b) \cdot z(a)} \\ &= \mathrm{Reg}_\lambda(\mathfrak{R}_\Sigma(E/K)) \cdot \frac{\#T_{\mathrm{loc}}}{\#T_{\mathrm{gl}} \cdot \#J \cdot [\mathfrak{R}(E/K) : \mathfrak{R}_\Sigma(E/K)]} \cdot \\ &\qquad \cdot \frac{\#(\mathcal{R}(E/K)/\operatorname{div})}{[\mathfrak{R}(E/K) : \mathfrak{R}_\Sigma(E/K)] \cdot \#I} \end{aligned}$$

If the regulator on $\mathfrak{R}_\Sigma(E/K)$ is replaced by $\mathrm{Reg}_\lambda(\mathfrak{R}(E/K))$ times the square of the index $[\mathfrak{R}(E/K) : \mathfrak{R}_\Sigma(E/K)]$, the index cancels from the formula. We obtain the formula in the theorem, which is now independent of the chosen set Σ. □

8. On the μ-invariant

Proposition 8.1. *Let E be an elliptic curve over $\mathbb{Q}$ which admits an isogeny defined over $\mathbb{Q}$ of degree p. Then the μ-invariant of the dual of $\mathcal{R}(E/_\infty\mathbb{Q})$ is zero.*

Proof. Let C the kernel of the isogeny. The fixed field K of the kernel of the map $\mathrm{Gal}(\bar{\mathbb{Q}} : \mathbb{Q}) \longrightarrow \mathrm{Aut}(C)$ is a cyclic extension of $\mathbb{Q}$ over which E admits a p-torsion point. By Corollary 3.6 of [5] this is enough to guarantee that the μ-invariant over K is trivial. (The proof relies on the theorem of Ferrero-Washington on the triviality of the classical μ-invariant.) The μ-invariant over $\mathbb{Q}$ can only be smaller. □

Coates and Sujatha made the following

Conjecture 8.2. *Let E/K be an elliptic curve over a number field. Then the μ-invariant of the fine Selmer group with respect to the cyclotomic $\mathbb{Z}_p$-extension is zero.*

We will see in the examples that our computation provide ample numerical evidence for this conjecture over $\mathbb{Q}$.

9. Curves of rank 0

In this and the following two sections, we wish to give several numerical examples in order to explain what one can obtain from the Euler-characteristic formula in Corollary 6.3. The curve E will always be defined over $\mathbb{Q}$ and we will frequently assume that the Tate-Shafarevich group is finite.

The first part is concerned with elliptic curves E of rank 0 over $\mathbb{Q}$. Since $\mathcal{M}(E/\mathbb{Q})$, contained in $E(\mathbb{Q}) \otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$, is trivial, we see that $\mathcal{R}(E/\mathbb{Q})$ is equal to $\mathcal{K}(E/\mathbb{Q})$. On the compact side, we know that $\mathfrak{R}(E/\mathbb{Q})$ is zero if and only $\mathcal{K}(E/\mathbb{Q})$ is finite; in which case, the group J is therefore nothing else but

$$J = \operatorname{coker}\big(\mathrm{cor}\colon {}_\infty H^1(E/\mathbb{Q})_\Gamma \longrightarrow H^1_\Sigma(\mathbb{Q}, T_pE)\big) = {}_\infty H^2(E/\mathbb{Q})^\Gamma.$$

Proposition 9.1. *Suppose* $Ш(E/\mathbb{Q})$ *is finite. If* $E(\mathbb{Q})$ *is finite but non-trivial, then* $\mathcal{R}(E/_\infty\mathbb{Q})$ *and* J *are trivial for all primes* $p > 7$ *not dividing* $\prod_\upsilon c_\upsilon$ *or* $\#Ш(E/\mathbb{Q})$.

Proof. For $p > 5$, we have $0 < \#\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p) < 2p$ by the theorem of Hasse-Weil. Since there is a point of finite order $1 < \ell \leqslant 7$ defined over $\mathbb{Q}$, the number of points in the reduction must be divisible by ℓ and hence can not be equal to p unless $\ell = p$. Therefore for a prime $p > 7$ dividing $\prod c_\upsilon$, there can not be a point of order p on $E(\mathbb{Q}_p)$. Hence the numerator in the first formula of Corollary 6.3 contains only factors which are not divisible by p. This formula only applies if E has potentially good reduction at p; but if not the numerator is still a bound on the product $\#J \cdot f_\mathcal{R}(0)$. Hence $\#J = f_\mathcal{R}(0) = 1$, and so $f_\mathcal{R} \in \Lambda^\times$ implies that $\mathcal{R}(E/\mathbb{Q})$ is finite.

Moreover we see from Proposition 4.1, we see that b is an isomorphism, i.e. $\mathcal{R}(E/\mathbb{Q})^\Gamma$ is trivial. This implies that $\mathcal{R}(E/_\infty\mathbb{Q})$ is trivial because it is finite. □

If there is no torsion point defined over $\mathbb{Q}$, then it is still true that the fine Selmer group over ${}_\infty\mathbb{Q}$ is most often trivial:

Proposition 9.2. *For an elliptic curve* $E/\mathbb{Q}$ *of rank 0 with finite* $Ш(E/\mathbb{Q})$*, there is a set of density of 1 of primes for which* $\mathcal{R}(E/_\infty\mathbb{Q})$ *is finite. If* E *admits an isogeny of degree* p *to a curve with a non-trivial torsion point, we may take the set to include all but a finite number of primes.*

Proof. The proof of Proposition 5.1 in Greenberg's part of [3] can be applied to the formula in Corollary 6.3. □

9.1. Numerical examples. It is quite traditional to consider as a first example the curves of conductor 11. They are given by the three equations

$$\begin{aligned} E_1\colon &\quad y^2 + y = x^3 - x^2 - 10\,x - 20 \\ E_2\colon &\quad y^2 + y = x^3 - x^2 - 7820\,x - 263580 \\ E_3\colon &\quad y^2 + y = x^3 - x^2 \end{aligned}$$

For all good, ordinary primes $p \neq 5$, the Selmer group $\mathcal{S}(E_i/_\infty\mathbb{Q})$ is trivial (see [4, Theorem 4.6]), and for all supersingular primes it is isomorphic to Λ (see [4, Theorem 4.5]). For $p = 5$, we have

$$\mathcal{S}(E_1/_\infty\mathbb{Q})^\wedge = \Lambda/(5) \qquad \mathcal{S}(E_2/_\infty\mathbb{Q})^\wedge = \Lambda/(5^2) \qquad \mathcal{S}(E_3/_\infty\mathbb{Q})^\wedge = 0$$

Proposition 9.3. *The fine Selmer groups $\mathcal{R}(E_i/_\infty\mathbb{Q})$ of the curves of conductor 11 are trivial for all odd primes p and all i, except for E_1 and $p = 5$ in which case it is finite but non-trivial and J contains 5 elements.*

Proof. It is known that the Tate-Shafarevich groups of the three curves E_i are trivial, see [17, Lemma VI.3]. Let p be a prime not dividing $2 \cdot 5 \cdot 11$ and, hence, of good reduction. The first formula in Corollary 6.3 gives

$$\#J \cdot f_{\mathcal{R}}(0) \equiv \#E_i(\mathbb{Q}_p)\{p\} \pmod{\mathbb{Z}_p^\times}$$

because the product of the Tamagawa factors is equal to 5 (for E_1 only) or 1 and there are no global p-torsion points for $p \neq 5$. On E_1 there is a rational 5-torsion point. This implies just as in the proof of Proposition 9.1 that $p \geqslant 7$ is non-anomalous, hence we can check that $E_i(\mathbb{Q}_p)\{p\}$ is trivial for all $p \neq 5$. So for all these primes J and $\mathcal{R}(E_i/_\infty\mathbb{Q})$ are trivial.

For $p = 11$, one can deduce that $\#J \cdot f_{\mathcal{R}}(0) = 1$ in the same manner, but using the formula in Theorem 6.1 which hold also for primes of bad reduction.

Finally for $p = 5$, we know that the characteristic power series of the Selmer groups are powers of 5. But 5 can not divide the series $f_{\mathcal{R}}$ by Proposition 8.1 because of the presence of isogenies of degree 5. Hence we have also here that $\mathcal{R}(E_i/_\infty\mathbb{Q})$ is finite. On the other hand, we compute that $\#J \cdot f_{\mathcal{R}}(0) = \#J$ is equal to 5 for E_1 and 1 for the other curves. For $i = 2$ and 3, Proposition 4.1 proves that $\mathcal{R}(E_i/_\infty\mathbb{Q})^\Gamma$ is trivial, whence so is $\mathcal{R}(E_i/_\infty\mathbb{Q})$. Meanwhile for $i = 1$ we have $\#\mathcal{R}(E_1/_\infty\mathbb{Q})^\Gamma = 5$. □

Another more complicated example is the curve 182D1 given by

$$E\colon \quad y^2 + x\,y + y = x^3 - x^2 + 3\,x - 5$$

and the prime $p = 5$. Unlike in the previous case we do not have an isogeny of degree p at our disposition. The Mordell-Weil group $E(\mathbb{Q})$ is trivial and the product $\prod c_v$ is equal to 1. The 5-primary part of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ can be verified to be trivial using the Heegner point over

the field $\mathbb{Q}(i)$. Although there is no 5-torsion point in $E(\mathbb{Q})$, there is one in $E(\mathbb{Q}_5)$, hence we have $\#J \cdot f_{\mathcal{R}}(0) = 5$. Even though we can not conclude whether $\mathcal{R}(E/_\infty\mathbb{Q})$ is finite or not, we can still decide that Conjecture 8.2 holds. Since $E[p]$ is an irreducible Galois-representation, the theorem of Kato shows that $f_{\mathcal{S}}$ divides the p-adic L-function. The invariants of this latter have been computed by Pollack [13] and he claims that $\mu_{\mathcal{S}} = 0$. Since $f_{\mathcal{R}}$ divides $f_{\mathcal{S}}$, we must have that $\mu_{\mathcal{R}} = 0$. The λ-invariant of the usual Selmer group equals at most 2.

10. Curves of rank 1

Compared to the computations for curves of rank 0, the only big difference is the presence of the term D in the formula in Corollary 6.3. Let E be the curve 37A1

$$E: \quad y^2 + y = x^3 - x.$$

It is known that $E(\mathbb{Q})$ is a free group generated by $P = (0, 0)$ and $Ш(E/\mathbb{Q}) = 0$, see [17, Lemma VI.5.]. We choose the good ordinary non-anomalous prime $p = 179$ which is the smallest prime for which D is non-trivial, see (6) in [19]. The formula gives now $\#J \cdot f_{\mathcal{R}}(0) = p$. But since the prime p has good ordinary reduction, we may use the Euler-characteristic formula (1.1) for the usual Selmer group and we get that $f^*_{\mathcal{S}}(0)$ is a unit and hence $f_{\mathcal{S}} = T$. Hence we can deduce that $f_{\mathcal{R}} = 1$ and that J has p elements. In particular $\mathcal{R}(E/_\infty\mathbb{Q})$ is finite but non-trivial. The same way one proves the following, see [17, Proposition VI.6.].

Proposition 10.1. *The fine Selmer group $\mathcal{R}(E/_\infty\mathbb{Q})$ for the curve* 37A1 *is finite for all odd primes $p < 1000$.*

We do not know anything about the distribution of primes p for a fixed elliptic curve E for which the group D is non-trivial. But it seems that for curves of rank 1, there might be an infinite set of such p but probably of density 0. Nevertheless even for these primes, the above method consisting of comparing with the usual Selmer group gives for most of them that the fine Selmer group $\mathcal{R}(E/_\infty\mathbb{Q})$ is finite. This is in support of the Conjecture 1.2. More computations can be found in [17, Table VI.2].

Here is a supersingular example:

$$E: \quad y^2 + x\,y + y = x^3 - x^2.$$

This is the curve labelled 53A1 whose Mordell-Weil group is generated by $P = (0, 0)$. Conjecturally the Tate-Shafarevich group is trivial; it can be shown with a 3-descent that $Ш(E/\mathbb{Q})[3]$ is trivial. We consider the supersingular

prime $p = 3$. There are no 3-torsion points on $E(\mathbb{Q}_3)$, but D is of order 3, because the first multiple of P in the kernel of reduction at 3 is $7 \cdot P = (\frac{40}{81}, -\frac{1025}{729})$ which is already in the second layer of the formal group. Hence $\#J \cdot f_{\mathcal{R}}(0) = 3$. Now, Pollack [13] computes for this example the Iwasawa invariants of the 3-adic analytic L-functions of the $+$ and $-$ Selmer groups as defined in [14]. They are both equal to T. Using Kobayashi's result [8] on the main conjecture in the supersingular context and that $f_{\mathcal{R}}$ has to divide both of these analytic L-function, we draw the conclusion that $f_{\mathcal{R}}$ is trivial and so $\mathcal{R}(E/_\infty\mathbb{Q})$ is, once again, finite.

11. Curves of rank $\geqslant 2$

The situation is similar to the rank 1 case. One more factor is appearing, due to the fact that the fine Selmer group $\mathcal{R}(E/\mathbb{Q})$ is no longer finite, namely the regulator. The non-degeneracy of the p-adic height implies that $\mathcal{R}(E/_\infty\mathbb{Q})$ is Λ-torsion. But over $\mathbb{Q}$ this is known unconditionally by the much celebrated theorem of Kato. We still need to compute the p-adic height for computing a bound on the leading coefficient $f^*_{\mathcal{R}}(0)$.

The methods for proving that the characteristic power series $f_{\mathcal{R}}$ is equal to T^r where r is the corank of $\mathcal{R}(E/\mathbb{Q})$ are the same as before : If the formula for $\#J \cdot f^*_{\mathcal{R}}(0)$ does not prove it, we will try to compare it with the classical formula (1.1) for $f^*_{\mathcal{S}}(0)$. The last possibilities would be to use either an isogeny of degree p, if there is one defined over $\mathbb{Q}$, or to use analytic computations by Pollack [13] and the divisibility of Kato. But all these methods are only useful to give upper bounds on the Iwasawa-invariants of $\mathcal{R}(E/_\infty\mathbb{Q})$. For tables and details of the computation, we refer the reader to [17, Table VI.3].

So far, we did not present any example in which the characteristic power series $f_{\mathcal{R}}$ is not simply a power of T. The last example gives now a curve with a different behaviour. In this case one can prove that the fine Selmer group has to grow because the rank of the fine Mordell-Weil group increases. There is no known example yet of an elliptic curve $E/\mathbb{Q}$ and a prime p for which the group $\text{Ш}(E/_\infty\mathbb{Q})$ is infinite. Compare this with the Question 8.3 in [19].

The following example is a rather complicated case for which the characteristic series of the fine Selmer group is not trivial. Let E be the curve 5692A1 given by

$$E: \quad y^2 = x^3 + x^2 - 18\,x + 25.$$

The Mordell-Weil group is a free group generated by the points $P_1 = (0, 5)$ and $P_2 = (1, 3)$. We are interested in this curve for the prime $p = 3$. It has

good ordinary, anomalous reduction at p, but $E(\mathbb{Q}_3)\{3\} = 0$. The analytic order of $Ш(E/\mathbb{Q})$ is 1 and the product of Tamagawa numbers is 3.

Assuming the triviality of the 3-primary part of the $Ш(E/\mathbb{Q})$, we get that the fine regulator has valuation 5 and the formula in Corollary 6.3 shows that $\#J \cdot f^*_{\mathcal{R}}(0)$ has valuation 6. Since it has ordinary reduction, we may compare with the characteristic series of the Selmer group. The first coefficient $f^*_{\mathcal{S}}(0)$ is 3^3 by (1.1) if $Ш(E/\mathbb{Q})$ has no 3-torsion.

Proposition 11.1. *Assume that the 3-primary part of* $Ш(E/\mathbb{Q})$ *is trivial. Then the characteristic power series of the Selmer group is equal to*

$$\begin{aligned} f_{\mathcal{S}} &= T^2 \cdot (3 + 3T + T^2)^2 \cdot (3 + 9T + 18T^2 + 21T^3 + 15T^4 + 6T^5 + T^6) \\ &= ((1+T)^3 - 1) \cdot ((1+T)^9 - 1) \end{aligned}$$

The characteristic power series for the dual of the fine Selmer group is

$$f_{\mathcal{R}} = T \cdot (3 + 3T + T^2) = (1+T)^3 - 1.$$

The group J contains 3^5 elements. In particular, we have that $E({}_\infty\mathbb{Q})$ has rank 12, $\mathfrak{M}(E/{}_\infty\mathbb{Q})$ has rank 3 and $Ш(E/{}_\infty\mathbb{Q})$ is finite.

Proof. Let ${}_1\mathbb{Q}$ be the first layer of the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$; it is generated by α satisfying $\alpha^3 - 3\alpha + 1 = 0$. With some luck, we were able to find six independent points in $E({}_1\mathbb{Q})$.

$$\begin{aligned} P_3 &= \quad (-\alpha^2 - 2\cdot\alpha + 2, -3\cdot\alpha^2 - 3\cdot\alpha + 4), \\ P_4 &= \quad (-\alpha^2 - 2\cdot\alpha + 3, -2\cdot\alpha^2 - 2\cdot\alpha), \\ P_5 &= (-2\cdot\alpha^2 - 3\cdot\alpha + 4, -\alpha^2 + 2), \\ P_6 &= (-2\cdot\alpha^2 - 2\cdot\alpha + 6, -2\cdot\alpha^2 + 2\cdot\alpha + 9). \end{aligned}$$

Hence the rank of $E({}_1\mathbb{Q})$ is at least 6. Next, we are looking at the second layer ${}_2\mathbb{Q}$ defined by β with $\beta^3 - 3\,\beta = \alpha$. Again we are lucky and find a point

$$\begin{aligned} P_7 = (&-\beta^6 + 7\cdot\beta^4 - \beta^3 - 14\cdot\beta^2 + 4\cdot\beta + 7, \\ &\beta^7 - 3\cdot\beta^6 - 7\cdot\beta^5 + 20\cdot\beta^4 + 11\cdot\beta^3 - 36\cdot\beta^2 + \beta + 15) \end{aligned}$$

which is linearly independent from the previous six points. The rank of $E({}_2\mathbb{Q})$ has to be at least 12.

The series $f_{\mathcal{S}}$ is therefore divisible by the right hand side of the formula in the proposition. Since $f^*_{\mathcal{S}}(0) = 3^3$, this divisibility must be an equality.

Because the rank of the Mordell-Weil group is jumping from $\operatorname{rank} E(\mathbb{Q}) = 2$ to $\operatorname{rank} E({}_1\mathbb{Q}) = 6$, it is clear that the fine Mordell-Weil group increases its rank from 1 to 3, in other words $(3 + 3T + T^2)$ divides exactly once $f_{\mathcal{R}}$. It is not possible that the last factor divides $f_{\mathcal{R}}$.

□

The analytic 3-adic L-function can be shown to be divisible by the three irreducible factors in the formula, but by no other distinguished polynomial or by p. I am thankful to Robert Pollack for this computation.

References

1. Dominique Bernardi, *Hauteur p-adique sur les courbes elliptiques*, Seminar on Number Theory, Paris 1979–80, Progr. Math., vol. 12, Birkhäuser Boston, 1981, pp. 1–14.
2. Dominique Bernardi and Bernadette Perrin-Riou, *Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 3, 227–232.
3. John Coates, Ralph Greenberg, Kenneth A. Ribet, and Karl Rubin, *Arithmetic theory of elliptic curves*, Lecture Notes in Mathematics, vol. 1716, Springer, 1999, Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997.
4. John Coates and Ramdorai Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 88, Narosa Publishing House, 2000.
5. ———, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), no. 4, 809 – 839.
6. Hideo Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions*, Proc. Japan Acad. **51** (1975), 12–16.
7. Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et application arithmétiques. III, Astérisque, vol. 295, Société Mathématique de France, Paris, 2004.
8. Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.
9. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2000.
10. Bernadette Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), no. 1, 137–185.
11. ———, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995.
12. ———, *Fonctions L p-adiques des représentations p-adiques*, Astérisque (1995), no. 229, 198.
13. Robert Pollack, *Iwasawa invariants of elliptic curves*, Available online at the address http://math.bu.edu/people/rpollack/Data/data.html.
14. ———, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.
15. Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.
16. Peter Schneider, *p-adic height pairings. II*, Invent. Math. **79** (1985), no. 2, 329–374.
17. Christian Wuthrich, *The fine Selmer group and height pairings*, Ph.D. thesis, University of Cambridge, UK, 2004.
18. ———, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) **70** (2004), no. 1, 23–40.
19. ———, *The fine Tate-Shafarevich group*, to appear in Math. Proc. Cambridge Philos. Soc., 2005.

Séction de mathématiques, CSAG, École polytechnique fédérale, 1015 Lausanne, Switzerland
E-mail address: christian.wuthrich@epfl.ch