J. Math. Soc. Japan
Vol. 53, No. 1, 2001

Euler characteristics and elliptic curves II

To the memory of Kenkichi Iwasawa.

By J. H. Coates and S. Howson*

(Received Aug. 13, 1999)
(Revised Oct. 4, 1999)

Abstract. This paper describes a generalisation of the methods of Iwasawa Theory to the field F_∞ obtained by adjoining the field of definition of all the p-power torsion points on an elliptic curve, E, to a number field, F. Everything considered is essentially well-known in the case E has complex multiplication, thus it is assumed throughout that E has no complex multiplication. Let G_∞ denote the Galois group of F_∞ over F. Then the main focus of this paper is on the study of the G_∞-cohomology of the p^∞-Selmer group of E over F_∞, and the calculation of its Euler characteristic, where possible. The paper also describes proposed natural analogues to this situation of the classical Iwasawa λ-invariant and the condition of having μ-invariant equal to 0.

The final section illustrates the general theory by a detailed discussion of the three elliptic curves of conductor 11, at the prime $p = 5$.

Let F be a finite extension of $\boldsymbol{Q}$, and E an elliptic curve defined over F. We assume throughout that *E has no complex multiplication* over the algebraic closure of F and we will make no further comment about this in the statement of our results. In fact, everything we shall consider is essentially well known in the complex multiplication case (see [**33**]). Let p be any prime number. Our aim is to consider a generalisation of the methods of Iwasawa Theory to the field F_∞ obtained by adjoining all the p-power torsion points on E to F. By a celebrated theorem of Serre [**41**], the Galois group G_∞ of F_∞ over F is isomorphic to an open subgroup of $GL_2(\boldsymbol{Z}_p)$, and hence is a non-Abelian, p-adic, Lie group of dimension four. This situation was first considered by M. Harris [**20**], [**22**], but remains shrouded in mystery today. We emphasize that the methods of classical Abelian Iwasawa Theory do not extend in any obvious fashion to the GL_2 theory, and that there are a number of obvious pitfalls if one follows such an approach (see [**1**].) We hope that our fragmentary results provide evidence that there is a deep and interesting Iwasawa theory to be discovered. We have largely concentrated on the study of the G_∞-cohomology of the p^∞-Selmer group of E over F_∞, and the calculation of its Euler characteristic

---

2000 *Mathematics Subject Classification*. 11G05, 11G40.
*Supported by a PhD grant from the E.P.S.R.C.

when these cohomology groups are all finite. In the classical theory of $\boldsymbol{Z}_p$-extensions an important role is played by Iwasawa's λ and μ-invariants for a torsion module over the Iwasawa algebra. In §6 we propose what seem to be natural analogues of the λ-invariant and having μ-invariant equal to 0 for the dual of the p^∞-Selmer group of E over F_∞ when we expect it to be torsion over the Iwasawa algebra of G_∞. (See also Greenberg [**17**], where a similar notion of having μ-invariant equal to 0 is introduced.) In §7 we illustrate our general theory by a detailed discussion of the three elliptic curves of conductor 11 and the prime $p = 5$, where we can prove all of our conjectures and calculate the analogue of the λ-invariant. We have not discussed at all the possible connexion of the p^∞-Selmer group of E over F_∞ with L-functions, although we strongly believe that such a link must exist.

1. Statement of main results.

For any algebraic extension, H, of F we define the p^∞-Selmer group of E over H, denoted $\mathcal{S}_p(E/H)$, in the usual way, that is by the exactness of the sequence

$$\mathcal{S}_p(E/H) = \mathrm{Ker}\left(H^1(H, E_{p^\infty}) \to \prod_\omega H^1(H_\omega, E) \right), \tag{1}$$

where ω runs over all places of H. Here, if H is an infinite extension of $\boldsymbol{Q}$ then H_ω denotes, as is usual, the union of the completions at ω of all finite extensions of $\boldsymbol{Q}$ contained in H. Denote by F_n the field obtained by just adjoining the p^{n+1}-torsion points on E to F. As remarked above, G_∞ is defined to be the Galois group of the field extension F_∞/F. Let G_n be the Galois group $\mathrm{Gal}(F_n/F)$. Then G_∞ can be embedded as a closed subgroup of $GL_2(\boldsymbol{Z}_p)$ and is thus a p-adic, Lie group. We define the *Iwasawa algebra* in this situation to be the following completed group algebra

$$\Lambda(G_\infty) = \varprojlim \boldsymbol{Z}_p[G_n] \tag{2}$$

where the inverse limit is taken with respect to the canonical projection maps.

Now G_∞ acts continuously on $\mathcal{S}_p(E/F_\infty)$, where this latter module is regarded as having the discrete topology, thus this action can be extended to a continuous action of $\Lambda(G_\infty)$ and it is generally more useful to regard $\mathcal{S}_p(E/F_\infty)$ as a $\Lambda(G_\infty)$-module. We consider also

$$\mathcal{C}_p(E/F_\infty) = \mathrm{Hom}(\mathcal{S}_p(E/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p) \tag{3}$$

which has the structure of a compact $\Lambda(G_\infty)$-module.

Because $\Lambda(G_\infty)$ generally contains zero divisors it is also convenient to fix a pro-p subgroup

$$R = \mathrm{Gal}(F_\infty/F_0), \text{ if } p > 2; \quad \mathrm{Gal}(F_\infty/F_1), \text{ if } p = 2. \tag{4}$$

By restricting to the action of R, any $\Lambda(G_\infty)$-module naturally has the structure of a $\Lambda(R)$-module, where $\Lambda(R)$ is defined analogously to $\Lambda(G_\infty)$. It is known that $\Lambda(R)$ has no zero divisors. We say that a $\Lambda(R)$-module, M, is $\Lambda(R)$-*torsion* if every element of M has a non-trivial annihilator in $\Lambda(R)$. Note that, because $\Lambda(R)$ is not Abelian, this is certainly weaker than asserting that M has a non-trivial global annihilator in $\Lambda(R)$.

One final piece of notation. If G is any profinite group which has finite p-cohomological dimension, n say, and if M is any p-primary Abelian group with the structure of a discrete G-module, then we define its *G-Euler Characteristic* by

$$\chi(G, M) = \prod_{0 \le i \le n} (\sharp H^i(G, M))^{(-1)^i} \tag{5}$$

if this is defined (i.e. all terms in the product are finite), otherwise we simply say the G-Euler Characteristic of M is undefined. Recall that the p-cohomological dimension of G, $\mathrm{cd}_p(G)$, is defined as the minimum number such that $H^i(G, M) = 0$ for all discrete, p-primary, G-modules, and for all $i > \mathrm{cd}_p(G)$. It is well known, [**38**], [**28**], that a p-adic, Lie group has p-cohomological dimension equal to its dimension as a p-adic manifold if it contains no element of order p, and infinite p-cohomological dimension otherwise. Thus our hypothesis on E implies that $\mathrm{cd}_p(G_\infty) = 4$ if $p \ge 5$ but can be infinite for $p = 2, 3$. This is the main, but not only, reason for excluding in particular the prime $p = 3$.

Then we prove the following:

THEOREM 1.1. *Let p be a rational prime such that* (i) $p \ge 5$, (ii) *E has good ordinary reduction at all places, v, of F dividing p,* (iii) *$\mathscr{S}_p(E/F)$ is finite and* (iv) *$\mathscr{C}_p(E/F_\infty)$ is $\Lambda(R)$-torsion. Then $\chi(G_\infty, \mathscr{S}_p(E/F_\infty))$ is defined and equals*

$$\rho_p(E/F) \times \left| \prod_{v \in \mathfrak{M}} L_v(E, 1) \right|_p, \tag{6}$$

where $\rho_p(E/F)$ is defined by

$$\rho_p(E/F) = \frac{\sharp Ш(E/F)(p) \prod_{v|p} ((\sharp \tilde{E}_v(k_{F_v})(p))^2)}{(\sharp E(F)(p))^2 \prod_{v \in S} |c_v|_p}. \tag{7}$$

Here, S is any finite set of places of F containing the Archimedean places and all primes of F which either divide p or where E has bad reduction. The set $\mathfrak{M}$

consists of the set of non-Archimedean places of F at which the classical j-invariant, j_E, of E is non-integral. Other terms in (7) will be defined at the beginning of §3. We simply note that it is finite, under our assumptions on E and p above. In fact, in section 5 we carry out all the local calculations necessary to prove a version of Theorem 1.1 replacing condition (ii) by the weaker statement (ii)′ E has potential good ordinary reduction at all places v of F dividing p. The formula for $\rho_p(E/F)$ then becomes somewhat more complicated to state, but it should be clear to anyone interested what form it takes, from the calculations in §5.

We should confess at this point that the exact formula for the corresponding result to Theorem 1.1 in our earlier note [**7**] is incorrect because of the omission of the mysterious term coming from the Euler factors of primes in $\mathfrak{M}$. We are grateful to Richard Taylor for pointing our earlier error out to us. We will discuss further the significance of these Euler factors later, when we carry out the local calculations.

THEOREM 1.2. *Under the hypotheses* (i) *and* (iv) *of Theorem* 1.1, *for every open subgroup* G *of* G_∞, *the cohomology groups* $H^i(G, \mathcal{S}_p(E/F_\infty))$ *are zero for all* $i \geq 2$.

Note in particular that we are assuming nothing about the structure of $\mathcal{S}_p(E/F)$, the p^∞-Selmer group over F, or, a priori, about the reduction type of E at p. (In fact, we shall prove that these cohomology groups vanish under a stronger condition, namely whenever $\mathcal{C}_p(E/F_\infty)$ satisfies Conjecture 2.4.)

More generally, we make the following conjectures:

CONJECTURE 1.3. *Under the condition on* p *that* E *has good ordinary reduction at all places of* F *dividing* p, $\mathcal{C}_p(E/F_\infty)$ *is always* $\Lambda(G_\infty)$*-torsion, and thus*

CONJECTURE 1.4. *Under conditions* (i), (ii) *and* (iii) *of Theorem* 1.1, $\chi(G_\infty, \mathcal{S}_p(E/F_\infty))$ *is defined and equals the value given in* (6) *and* (7).

Conjecture 1.3 was first made by M. Harris in [**19**] (see also the correction [**22**]). A more general conjecture, taking into account the behaviour of supersingular primes, is given in the next section. This also allows us to conjecture more generally when Theorem 1.2 should hold. Currently our evidence for this conjecture is rather slight. It consists principally of a very weak theorem which follows from a discussion of the relationship between Conjecture 1.3 and the corresponding conjecture in the theory for the cyclotomic $\boldsymbol{Z}_p$-extension. We will describe what we can currently say about the relationship between the two situations in some detail in §6. Using this relationship we are able to prove all of our conjectures for a small number of numerical examples, including the three curves of conductor 11 and the prime $p = 5$. Our proofs are based on descent

calculations for these elliptic curves over the field $\boldsymbol{Q}(\mu_p)$, due to R. Greenberg (see [**10**] for an account of Greenberg's work, which is announced in [**17**]), and more recently to T. Fisher (unpublished). We will give a brief summary of these calculations and the examples which follow in the final section. Our other main evidence is an explicit upper bound on just how large the rank of $\mathscr{C}_p(E/F_\infty)$ as a $\Lambda(G_\infty)$-module can be, given in [**25**] and [**24**]. The main motivation for Conjecture 1.3 is by analogy with the classical situation of the cyclotomic $\boldsymbol{Z}_p$-extension of F, where the corresponding conjecture (originally due to Mazur, see [**29**]) is long standing, and has recently been proven for E modular, defined over $\boldsymbol{Q}$ and with $F/\boldsymbol{Q}$ Abelian, by Kato [**26**]. A similar statement to Conjecture 1.4 is a well known theorem in this case, but the value of the Euler characteristic is then just $\rho_p(E/F)$, without the Euler factors at primes of non-integral j-invariant.

Due to the sparsity of explicit examples where Conjecture 1.3 is known to hold, we will also establish a partial result in the direction of Theorem 1.1, which holds without any assumption on the structure of $\mathscr{C}_p(E/F_\infty)$ as a $\Lambda(G_\infty)$-module. In the potential good, ordinary case, however, we can establish nothing in the direction of Theorem 1.2 without knowing the torsion of $\mathscr{C}_p(E/F_\infty)$.

In an appendix we will also give a proof of the following result, the truth of which was pointed out to us by R. Greenberg.

THEOREM 1.5. *Assume* $p \geq 5$. *Then*

$$\dim_{\boldsymbol{Q}_p}(\mathscr{C}_p(E/F_\infty) \otimes_{\boldsymbol{Z}_p} \boldsymbol{Q}_p) = \infty. \tag{8}$$

In other words, the p^∞-Selmer group is 'large' despite Conjecture 1.3. Note that, unlike in the classical cyclotomic situation, Theorem 1.5 is not incompatible with Conjecture 1.3. The hypothesis $p \geq 5$ is only necessary in case E has unstable reduction and integral j-invariant at all primes of F dividing p. We believe that Theorem 1.5 is true for all primes p without restriction.

Our proof of Theorem 1.5 gives no indication as to whether the size of $\mathscr{C}_p(E/F_\infty)$ is due to a large Mordell-Weil group over F_∞ or a large Tate-Shafarevič group, $Ш(E/F_\infty)$. This is something which would be extremely interesting to clarify (presumably both can be large.) Under certain conditions (including assuming E has good ordinary reduction at all primes v of F dividing p) Theorem 1.5 follows from work of Harris in [**21**], where he actually constructs explicit lower bounds on the Mordell-Weil rank of E over F_n.

Our motivation for studying Theorem 1.1 is the following. Exact formulae play an important part in the Iwasawa Theory of elliptic curves. If the p^∞-Selmer group at the F_∞ level is to eventually be useful in studying the arithmetic of E over the base field, F, we must be able to recover the basic arithmetic invariants of E over F from some formula related to the $\Lambda(R)$-module structure of $\mathscr{S}_p(E/F_\infty)$. In the classical analogue of our theory over the cyclotomic $\boldsymbol{Z}_p$-

extension of F, Theorem 1.1, when combined with an Iwasawa Main Conjecture, is what would be expected from a p-adic Birch and Swinnerton-Dyer conjecture, as described in [**30**] and gives information about the original conjecture of Birch and Swinnerton-Dyer. In fact, it largely motivated the formulation of the p-adic Birch and Swinnerton-Dyer conjecture. For elliptic curves admitting complex multiplication, such a Main Conjecture has been proven by Rubin and Yager. In the setting of this paper we do not yet have the tools available to formulate an analogous Main Conjecture. So we study such explicit formulae directly instead. Further discussion of this motivation was given in our earlier paper [**7**]. We note that a preliminary account of the results of this paper is also given in the lectures [**4**].

NOTATION. The following notation is used throughout:

- If A is any Abelian group then $A(p)$ denotes its p-primary subgroup.
- If S is any finite set of primes of F then F^S denotes the maximal extension of F unramified outside S.
- If A is either a discrete p-primary Abelian group or a compact pro-p group then the Pontrjagin dual of A is defined by

$$\hat{A} = \mathrm{Hom}(A, \boldsymbol{Q}_p/\boldsymbol{Z}_p).$$

- For an elliptic curve, E, defined over F, F_∞ throughout denotes the extension of F obtained by adjoining all the p-power torsion points on E, and F^{cyc} denotes the cyclotomic $\boldsymbol{Z}_p$-extension of F.
- The Galois group of F_∞ over F is denoted by G_∞ and R is a fixed pro-p subgroup of G_∞ defined by (4).

ACKNOWLEDGEMENTS. We would like to warmly thank R. Greenberg for many helpful conversations and contributions to the contents of this paper. We would also like to thank J-P. Serre for providing us with a proof of Theorem 4.2, R. Sujatha for first pointing out the finiteness of the cohomology groups in (131), and Y-H. Ochi, R. L. Taylor and B. Totaro for making a number of helpful observations while this work was in progress.

2. Preliminaries.

We will need certain general results about the algebraic structure of $\Lambda(R)$ and finitely generated $\Lambda(R)$-modules which are collected together here for reference. By a $\Lambda(R)$-module we will always mean a *left* $\Lambda(R)$-module. So long as we are consistent, though, we could of course equally well talk about right $\Lambda(R)$-modules.

The action of G_∞ on E_{p^∞} defines a canonical representation

$$\rho : G_\infty \hookrightarrow \mathrm{Aut}(E_{p^\infty}) \xrightarrow{\sim} GL_2(\boldsymbol{Z}_p). \tag{9}$$

When there is no danger of confusion, we shall drop the homomorphism ρ from the notation, and identify G_∞ with a subgroup of $GL_2(\boldsymbol{Z}_p)$. Note that ρ maps R into the subgroup of $GL_2(\boldsymbol{Z}_p)$ consisting of all matrices which are congruent to the identity modulo p if $p \geq 3$, 4 if $p = 2$. In particular, it follows that R is always a pro-p group. However, it is not in general true that G_∞ itself is a pro-p group. The following fundamental result about the size of G_∞ is due to Serre [**41**].

THEOREM 2.1. i) *G_∞ is open in $GL_2(\boldsymbol{Z}_p)$ for all primes p, and*
ii) *$G_\infty = GL_2(\boldsymbol{Z}_p)$ for all but a finite number of primes p.*

The following is an extension, due to Serre [**38**], of a theorem of Lazard [**28**].

THEOREM 2.2. *Any p-adic, Lie group, G, containing no element of order p has finite p-cohomological dimension which is equal to its dimension as a p-adic manifold.*

By virtue of Theorem 2.1, G_∞ is a p-adic Lie group of dimension 4. Thus G_∞ will have p-cohomological dimension equal to 4 provided G_∞ has no p-torsion. Since G_∞ is a subgroup of $GL_2(\boldsymbol{Z}_p)$, it will certainly have no p-torsion provided $p \geq 5$.

The final algebraic property we need is

THEOREM 2.3. *The Iwasawa algebra $\Lambda(R)$ is left and right Noetherian and has no divisors of zero.*

This is a special case of a theorem of Lazard's [**28**].

It is known (see [**13**] chapter 9) that Theorem 2.3 implies that $\Lambda(R)$ admits a skew field of fractions, which we denote by $K(R)$. If M is any finitely generated $\Lambda(R)$-module then we define the $\Lambda(R)$-rank of M by

DEFINITION.

$$\Lambda(R)\text{-rank}(M) = \dim_{K(R)}(K(R) \otimes_{\Lambda(R)} M) \tag{10}$$

Note that the theory of vector spaces over skew fields exactly parallels the usual theory in the Abelian case, so this definition is a valid one. What is more, since $K(R)$ is a flat $\Lambda(R)$-module, $\Lambda(R)$-rank is additive with respect to exact sequences of finitely generated $\Lambda(R)$-modules. As would be expected, M is torsion in the sense defined previously if and only if the $\Lambda(R)$-rank of M is zero.

For each prime, v dividing p, of F define the integer $\tau_v(E/F)$ by

$$\tau_v(E/F) = \begin{cases} |F_v : \boldsymbol{Q}_p| & \text{if } E \text{ has potential} \\ & \text{supersingular reduction at } v, \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

Put

$$\tau_p(E/F) = \sum_{v|p} \tau_v(E/F) \tag{12}$$

We can now make the more general conjecture about the size of $\mathcal{C}_p(E/F_\infty)$ promised in the previous section.

CONJECTURE 2.4. *For every prime, p, the $\Lambda(R)$-rank of $\mathcal{C}_p(E/F_\infty)$ is equal to*

$$\tau_p(E/F)|G_\infty : R|.$$

Since, of course, $\tau_p(E/F) = 0$ if E has good ordinary reduction at all primes of F dividing p, this incorporates the earlier Conjecture 1.3 made above.

For interest, we quote here the following from [**25**], [**24**].

THEOREM 2.5. *For all primes $p \geq 5$ we have*

$$\tau_p(E/F) \leq \frac{\Lambda(R)\text{-rank}(\mathcal{C}_p(E/F_\infty))}{|G_\infty : R|} \leq |F : \boldsymbol{Q}| \tag{13}$$

Let G now be any p-adic, Lie group. Recall the augmentation ideal of $\Lambda(G)$ is defined by

$$I(G) = \text{Ker}(\Lambda(G) \to \boldsymbol{Z}_p) \tag{14}$$

Here $\Lambda(G)$ is defined, for any p-adic Lie group, as in (2). Then the following essentially well known theorem is discussed in [**1**]

THEOREM 2.6 (Nakayama's Lemma). *Assume that G is a pro-p, p-adic, Lie group, and that M is a compact, left $\Lambda(G)$-module. Then $M = 0$ if and only if $M/I(G)M = 0$. It follows that if $M/I(G)M$ is a finitely generated $\boldsymbol{Z}_p$-module, then M is a finitely generated $\Lambda(G)$-module.*

Clearly any $\Lambda(G_\infty)$-module which is finitely generated as a $\Lambda(R)$-module is also finitely generated as a $\Lambda(G_\infty)$-module.

It is interesting to note that the stronger version of Nakayama's lemma, giving a useful criterion for M to be $\Lambda(G)$-torsion, does not generalise to arbitrary pro-p, p-adic, Lie groups. See [**1**] a discussion of what can be said.

We now turn to some preliminary steps in the proof of Theorems 1.1 and 1.2. Recall S is any finite set of primes of F containing the set of primes dividing p, the primes of bad reduction and the Archimedean primes and F^S denotes the maximal extension of F which is unramified outside the set S. Then F^S contains F_∞. It is well known that this implies the p^∞-Selmer group (over any field contained in F^S) can be defined by considering local conditions only at

the primes dividing those in S. Because of our assumption that $p \neq 2$ we may also ignore all local considerations at infinite primes.

Define

$$J_v(F_\infty) = \varinjlim \bigoplus_{\omega_n | v} H^1(F_{n,\omega_n}, E)(p) \tag{15}$$

where the limit is taken with respect to the restriction maps. For each n, the ω_n range over the primes of F_n which lie above v, and F_{n,ω_n} denotes the completion of F_n at ω_n. Thus we obtain the following fundamental diagram with exact rows.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{S}_p(E/F_\infty)^{G_\infty} & \longrightarrow & H^1(F^S/F_\infty, E_{p^\infty})^{G_\infty} & \xrightarrow{\psi_\infty} & \left(\bigoplus_{v\in S} J_v(F_\infty)\right)^{G_\infty} \\
 & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \delta=\oplus\delta_v} \\
0 & \longrightarrow & \mathcal{S}_p(E/F) & \longrightarrow & H^1(F^S/F, E_{p^\infty}) & \xrightarrow{\lambda_F} & \bigoplus_{v\in S} H^1(F_v, E)(p)
\end{array} \tag{16}$$

The vertical maps are given by restriction maps. It is by a detailed analysis of this diagram that we will be able to prove Theorems 1.1 and 1.2.

The following well known lemma (see [**8**]), whose proof we omit, describes the cokernel of λ_F when $\mathcal{S}_p(E/F)$ is finite.

LEMMA 2.7. *Let p be an odd prime and assume that $\mathcal{S}_p(E/F)$ is finite. Then* $\mathrm{Coker}(\lambda_F) = \widehat{E(F)(p)}$.

The inflation-restriction sequence in Galois cohomology describes the kernels and cokernels of β and δ. We have the exact sequence

$$\begin{aligned} 0 \to H^1(G_\infty, E_{p^\infty}) \to H^1(F^S/F, E_{p^\infty}) &\xrightarrow{\beta} H^1(F^S/F_\infty, E_{p^\infty})^{G_\infty} \\ &\to H^2(G_\infty, E_{p^\infty}) \to H^2(F^S/F, E_{p^\infty}) \end{aligned} \tag{17}$$

and thus $\mathrm{Ker}(\beta)$, $\mathrm{Coker}(\beta)$ are both finite independent of any hypothesis on E, p, as was first pointed out by Serre in [**37**], [**40**]. We will explain this later, see Lemma 4.1.

Turning to the local maps, we first require

LEMMA 2.8. *For each prime v in S let ω be any prime of F_∞ dividing v. Then $H^i(G_\infty, J_v(F_\infty))$ is canonically isomorphic to $H^i(\Delta_\omega, H^1(F_{\infty,\omega}, E)(p))$, where Δ_ω is the decomposition group of G_∞ at ω.*

By a prime of F_∞ we shall mean a compatible sequence of primes for each finite extension of F contained in F_∞. It is sufficient just to consider the sub-extensions F_n. Then $\omega = (\omega_n)$, where the ω_n satisfy $\omega_{n+1}|\omega_n$. This is equivalent to the usual notion of a prime of F_∞. To say that ω divides v means simply that each $\omega_n|v$. We then have

$$F_{\infty,\omega} = \bigcup_n F_{n,\omega_n} \tag{18}$$

We omit the proof of the above lemma, which follows immediately from Shapiro's lemma as in prop. 7.2 chap. VII of [**3**].

Now we can give the local analogue of (17). For each v in S, we have an exact sequence

$$\begin{aligned} 0 \to H^1(\Delta_\omega, E(F_{\infty,\omega}))(p) \to H^1(F_v, E)(p) \xrightarrow{\delta_v} H^1(F_{\infty,\omega}, E)(p)^{\Delta_v} \\ \to H^2(\Delta_\omega, E(F_{\infty,\omega}))(p) \to H^2(F_v, E)(p) \end{aligned} \tag{19}$$

describing $\mathrm{Ker}(\delta_v)$, $\mathrm{Coker}(\delta_v)$. In fact $H^2(F_v, E)(p) = 0$.

The snake lemma applied to the fundamental diagram (16) gives the following exact sequence

$$\begin{aligned} 0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta) \to \mathrm{Ker}(\delta) \cap \mathrm{im}(\lambda_F) \to \mathrm{Coker}(\alpha) \\ \to \mathrm{Coker}(\beta) \to \mathrm{im}(\psi_\infty)/\delta(\mathrm{im}(\lambda_F)) \to 0. \end{aligned} \tag{20}$$

We can thus immediately conclude

THEOREM 2.9. *The kernel of α is finite and the Pontrjagin dual of the cokernel is finitely generated as a $\boldsymbol{Z}_p$-module. Thus*

i) *$\mathscr{C}_p(E/F_\infty)$ is a finitely generated $\Lambda(R)$-module, and*

ii) *the Pontrjagin dual of $H^1(F^S/F_\infty, E_{p^\infty})$ is a finitely generated $\Lambda(R)$-module.*

PROOF. Diagram (16) holds with any choice of ground field, thus we may take

$$F = F_0 = F(E_p), p > 2; \quad F = F_1 = F(E_4), p = 2.$$

Firstly, since $\mathrm{Ker}(\beta)$ is finite $\mathrm{Ker}(\alpha)$ is finite also. Also, we know that

$$\mathrm{Ker}(\delta) \subset \bigoplus_{v \in S} H^1(F_v, E)(p)$$

By Tate local duality the Pontrjagin dual of each $H^1(F_v, E)(p)$ is $E(F_v)\hat{\otimes}\boldsymbol{Z}_p$, a finitely generated $\boldsymbol{Z}_p$-module (of rank 0 if $v \nmid p$, rank $|F_v : \boldsymbol{Q}_p|$ if $v|p$) and so $\mathrm{Ker}(\delta)$ is cofinitely generated as a $\boldsymbol{Z}_p$-module. It follows that the same is true

of Coker(α). But $\mathcal{S}_p(E/F)$ is a subgroup of $H^1(F^S/F, E_{p^\infty})$ which is cofinitely generated as a $\boldsymbol{Z}_p$-module (due to Tate, see [**31**] Corollary 4.15.) Thus $\mathcal{S}_p(E/F)$ is itself cofinitely generated as a $\boldsymbol{Z}_p$-module. It follows that $\mathcal{C}_p(E/F_\infty)_R$, the R-coinvariants of $\mathcal{C}_p(E/F_\infty)$, is a finitely generated $\boldsymbol{Z}_p$-module. Since $\mathcal{C}_p(E/F_\infty)$ is the Pontrjagin dual of $\mathcal{S}_p(E/F_\infty)$, a discrete $\Lambda(R)$-module, and thus is itself a compact $\Lambda(R)$-module, part (i) of the theorem then follows by Nakayama's lemma, 2.6. Similarly, since Coker(β) is finite, it follows that $H^1(F^S/F_\infty, E_{p^\infty})^R$ is cofinitely generated as a $\Lambda(R)$-module. Since $H^1(F^S/F_\infty, E_{p^\infty})$ is discrete, the second part also then follows from 2.6. □

We are grateful to Y. Ochi ([**32**]) for pointing out to us the following which is particularly interesting as the first real example of a result which is actually easier to prove in this non-Abelian situation.

THEOREM 2.10. *For all odd primes p, we have*

$$H^2(F^S/F_\infty, E_{p^\infty}) = 0. \tag{21}$$

Indeed, for F^{cyc} the cyclotomic $\boldsymbol{Z}_p$-extension of F, it has long been conjectured that

$$H^2(F^S/F^{cyc}, E_{p^\infty}) = 0 \tag{22}$$

for all odd primes p. However, at present this latter assertion has only been proven in some rather special cases. Theorem 2.10 is not necessary in the proof of Theorems 1.1 and 1.2 as stated above as in fact it would follow from the assumption that $\mathcal{C}_p(E/F_\infty)$ is $\Lambda(R)$-torsion. It is, however, necessary for the proof of part (ii) of Prop 3.1, part of the strongest result we can prove without any version of the rank Conjecture, 2.4.

We will not give the full proof of Theorem 2.10. We simply note that since E_{p^∞} is rational over F_∞ the Galois group Gal(F^S/F_∞) operates trivially on E_{p^∞} and so it is sufficient to show (21) with E_{p^∞} replaced by $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. However, because F_∞ contains all the p^{th}-power roots of unity (due to the Weil pairing) this is equivalent to

$$\varinjlim H^2(F^S/F_n(\mu_{p^\infty}), \boldsymbol{Q}_p/\boldsymbol{Z}_p) = 0. \tag{23}$$

But each term in this inductive limit is known to be zero, by virtue of a classical result due to Iwasawa.

3. Proofs of theorems 1.1 and 1.2.

In this section we give proofs of Theorems 1.1 and 1.2 subject to the statement of certain results concerning the local and global Galois cohomology of the field F_∞ which will be established in the next two sections.

We start by defining all the terms appearing in formulae (6) and (7).

• $Ш(E/F)$ is the Tate-Shafarevič group of E over F.

For each finite prime, v of F:

• $c_v = |E(F_v) : E_0(F_v)|$ denotes the local Tamagawa factor at v, (recall $E_0(F_v)$ is the subgroup of $E(F_v)$ consisting of the points with non-singular reduction at v.)

• $L_v(E, s)$ denotes the Euler factor of E at v.

• Write k_{F_v} for the residue field of F at v, and $\tilde{E}_v$ for the reduction of E over F_v, if E has good reduction at v. In this case, $\tilde{E}_{v,p^\infty}$ will denote the p-primary subgroup of $\tilde{E}_v(\overline{k_{F_v}})$.

Due to the sparsity of examples where the rank Conjecture 2.4 is known, we start by proving the strongest result we can in the direction of Theorem 1.1 without assuming that $\mathscr{C}_p(E/F_\infty)$ is $\Lambda(R)$-torsion.

PROPOSITION 3.1. *Assume $p \geq 3$ and j_E is integral at all v dividing p. Then the group $H^0(G_\infty, \mathscr{S}_p(E/F_\infty))$ is finite if and only if both $\mathscr{S}_p(E/F)$ is finite and $\tau_p(E/F) = 0$. In this case*

i) *both $H^1(G_\infty, \mathscr{S}_p(E/F_\infty))$ and the cokernel of the map ψ_∞ appearing in the fundamental diagram* (16) *are finite*;

ii) *they satisfy*

$$\sharp H^1(G_\infty, \mathscr{S}_p(E/F_\infty)) \quad \textit{divides} \quad \sharp\mathrm{Coker}(\psi_\infty)\sharp H^3(G_\infty, E_{p^\infty}). \tag{24}$$

We will prove this together with the next proposition, obtaining formulae relating the quantities appearing in the proposition which can then be made more explicit if we strengthen the hypotheses on the reduction type of E at primes dividing p. The reason for having to include the second condition, that j_E is integral at $v|p$, is the following: it is conjectured that $\mathrm{Ker}(\delta_v)$, $\mathrm{Coker}(\delta_v)$ are finite for v dividing p such that j_E is not integral, but it is currently unknown in general. Since we need this in the proof of the proposition, we cannot include this case. More generally, we conjecture

CONJECTURE 3.2. *For each $p \geq 5$, $\chi(G_\infty, \mathscr{S}_p(E/F_\infty))$ is defined if and only if both*

i) *$\mathscr{S}_p(E/F)$ is finite and*

ii) *$\tau_p(E/F) = 0$.*

We shall see in the proof of Proposition 3.1 that even the finiteness of $H^0(G_\infty, \mathscr{S}_p(E/F_\infty))$ implies that $\mathscr{S}_p(E/F)$ is finite and $\tau_p(E/F) = 0$. It is the converse which is currently mysterious, resting upon a proof of the case $\tau_p(E/F) = 0$ of Conjecture 2.4, together with a positive answer to the question mentioned above about the finiteness of $\mathrm{Ker}(\delta_v)$, $\mathrm{Coker}(\delta_v)$ when $ord_v(j_E) < 0$.

To get an exact formula, we simplify to the case where E has stable reduction at all primes of F dividing p. As remarked above, this is not strictly necessary but it does make the statement of the formula much simpler.

PROPOSITION 3.3. *If $p \geq 5$ and E has good ordinary reduction at all primes of F dividing p, and if $\mathcal{S}_p(E/F)$ is finite, then the cardinalities of* $\mathrm{Coker}(\psi_\infty)$ *and* $H^0(G_\infty, \mathcal{S}_p(E/F_\infty))$ *are related by the formula*

$$\sharp H^0(G_\infty, \mathcal{S}_p(E/F_\infty)) = \sharp H^3(G_\infty, E_{p^\infty}) \sharp \mathrm{Coker}(\psi_\infty) \rho_p(E/F) \left| \prod_{v \in \mathfrak{M}} L_v(E,1) \right|_p \tag{25}$$

PROOF. The first easy remark is that if $H^0(G_\infty, \mathcal{S}_p(E/F_\infty))$ is finite then $\mathcal{S}_p(E/F)$ must be also. This is clear because, by Theorem 2.9, the kernel of the map

$$\alpha : \mathcal{S}_p(E/F) \to \mathcal{S}_p(E/F_\infty)^{G_\infty} \tag{26}$$

is finite. Consider, now, the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{im}(\psi_\infty) & \longrightarrow & \left(\bigoplus_{v \in S} J_v(F_\infty) \right)^{G_\infty} & \longrightarrow & \mathrm{Coker}(\psi_\infty) & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \delta_1} & & \delta = \uparrow{\scriptstyle \oplus \delta_v} & & \uparrow{\scriptstyle \eta} & & \\ 0 & \longrightarrow & \mathrm{im}(\lambda_F) & \longrightarrow & \bigoplus_{v \in S} H^1(F_v, E)(p) & \longrightarrow & \mathrm{Coker}(\lambda_F) & \longrightarrow & 0 \end{array} \tag{27}$$

Here, $\mathrm{Ker}(\delta_1) = \mathrm{Ker}(\delta) \cap \mathrm{im}(\lambda_F)$ and $\mathrm{Coker}(\delta_1) = \mathrm{im}(\psi_\infty)/(\delta(\mathrm{im}(\lambda_F)))$.

But from the fundamental diagram, (16), and the exact sequence it gives, (20), the assumption that $\mathrm{Coker}(\alpha)$ is finite implies that $\mathrm{Ker}(\delta_1)$ and $\mathrm{Coker}(\delta_1)$ are both finite. Since, by Lemma 2.7 and our assumption that $p \geq 3$, $\mathrm{Coker}(\lambda_F)$ is finite, this implies that $\mathrm{Ker}(\delta)$ must be finite. But, we will see in Lemma 5.17 that $\mathrm{Ker}(\delta_v)$ is infinite if E has potential supersingular reduction at v for some v dividing p. Since, by definition (11), $\tau_v(E/F)$ is non-zero if and only if E has potential supersingular reduction at v, it follows that $\tau_p(E/F)$ must be zero.

The argument up until now has not required the hypothesis that j_E is integral at all v dividing p. We need this for the converse. Suppose $\tau_p(E/F) = 0$ and $\mathcal{S}_p(E/F)$ is finite. Then, by Proposition 5.12 for primes not dividing p, Corollary 5.22 for primes dividing p and Lemma 2.7, $\mathrm{Ker}(\delta)$, $\mathrm{Coker}(\delta)$ and $\mathrm{Coker}(\lambda_F)$ are all finite. By the snake lemma applied to diagram (27) above, we find (i) $\mathrm{Coker}(\eta)$ is finite and thus $\mathrm{Coker}(\psi_\infty)$ is finite and (ii)

$$\frac{\sharp \mathrm{Ker}(\delta_1)}{\sharp \mathrm{Coker}(\delta_1)} = \frac{\sharp \mathrm{Ker}(\delta)}{\sharp \mathrm{Coker}(\delta)} \times \frac{\sharp \mathrm{Coker}(\psi_\infty)}{\sharp \mathrm{Coker}(\lambda_F)} \tag{28}$$

By (20) this implies that $\mathrm{Coker}(\alpha)$ is finite and thus so is $H^0(G_\infty, \mathscr{S}_p(E/F_\infty))$. This completes the proof of the first statement in Proposition 3.1. But in fact, taking alternating products along the sequence (20), we get the explicit formula

$$\sharp H^0(G_\infty, \mathscr{S}_p(E/F_\infty)) = \frac{\sharp\mathrm{Ker}(\delta)}{\sharp\mathrm{Coker}(\delta)} \times \frac{\sharp\mathrm{Coker}(\beta)}{\sharp\mathrm{Ker}(\beta)} \times \frac{\sharp\mathrm{Coker}(\psi_\infty)}{\sharp\mathrm{Coker}(\lambda_F)} \times \sharp\mathscr{S}_p(E/F). \quad (29)$$

We now substitute in the information from sequence (17) which, together with Lemma 4.3, describes the kernel and cokernel of β, the information from Lemma 2.7 describing the cokernel of λ_F, and the fact that $\sharp\mathscr{S}_p(E/F) = \sharp Ш(E/F)(p)$. This gives

$$\sharp H^0(G_\infty, \mathscr{S}_p(E/F_\infty)) = \frac{\sharp\mathrm{Ker}(\delta)}{\sharp\mathrm{Coker}(\delta)} \times \frac{\sharp H^2(G_\infty, E_{p^\infty})}{\sharp H^1(G_\infty, E_{p^\infty})} \times \frac{\sharp\mathrm{Coker}(\psi_\infty)}{\sharp E(F)(p)} \times \sharp Ш(E/F)(p). \quad (30)$$

We now add the extra hypothesis of Proposition 3.3, that E actually has good (not just potential good) ordinary reduction at all the primes of F dividing p. Then we can identify the term coming from the local maps explicitly. This is given in Proposition 5.12 for primes not dividing p. For primes dividing p the value of this term is given in Corollary 5.26. Substituting this information in, we obtain

$$\sharp H^0(G_\infty, \mathscr{S}_p(E/F_\infty)) = \frac{\sharp H^2(G_\infty, E_{p^\infty})}{\sharp H^1(G_\infty, E_{p^\infty})} \times \sharp H^0(G_\infty, E_{p^\infty}) \times \frac{\rho_p(E/F)\sharp\mathrm{Coker}(\psi_\infty)\left|\prod_{v\in\mathfrak{M}} L_v(E,1)\right|_p}{\prod_{v|p}\left(\prod_{0\le i\le 2} \sharp H^i(\Delta_\omega, \tilde{E}_{v,p^\infty})^{(-1)^i}\right)}. \quad (31)$$

From the global and local Euler characteristic theorems, (4.2 and equation (118) in Proposition 5.26) proved in the next two sections, we see that the right hand side of (31) is

$$= \sharp H^3(G_\infty, E_{p^\infty})\sharp\mathrm{Coker}(\psi_\infty)\rho_p(E/F)\left|\prod_{v\in\mathfrak{M}} L_v(E,1)\right|_p \quad (32)$$

as required for the Proposition 3.3.

The final remark we need to make is that the finiteness of $\mathscr{S}_p(E/F)$ and $\mathrm{Coker}(\psi_\infty)$ implies $H^1(G_\infty, \mathscr{S}_p(E/F_\infty))$ is also finite. We no longer need the hypothesis that E has stable reduction at all v dividing p. Suppose X is the

image of $H^1(F^S/F_\infty, E_{p^\infty})$ under the localisation maps, so for some $\Lambda(R)$-module Y, the sequences

$$0 \to \mathcal{S}_p(E/F_\infty) \to H^1(F^S/F_\infty, F_{p^\infty}) \to X \to 0 \tag{33}$$

$$0 \to X \to \prod_{v \in S} J_v(F_\infty) \to Y \to 0 \tag{34}$$

are exact. This gives the following commutative, exact diagram:

$$\begin{array}{ccccccc} & & 0 & & & & \\ & & \downarrow & & & & \\ H^1(F^S/F_\infty, E_{p^\infty})^{G_\infty} & \xrightarrow{\varepsilon} & X^{G_\infty} & \longrightarrow & H^1(G_\infty, \mathcal{S}_p(E/F_\infty)) & \longrightarrow & H^3(G_\infty, E_{p^\infty}) \\ & & \downarrow & & & & \\ & & \left(\bigoplus_{v \in S} J_v(F_\infty)\right)^{G_\infty} & & & & \end{array} \tag{35}$$

Thus if $\mathrm{Coker}(\psi_\infty)$ is finite then so also is $\mathrm{Coker}(\varepsilon)$. We have $H^3(G_\infty, E_{p^\infty})$ on the right because, by Lemma 4.4 of the next section, $H^1(G_\infty, H^1(F^S/F_\infty, E_{p^\infty}))$ is isomorphic to $H^3(G_\infty, E_{p^\infty})$. This is finite. Thus $H^1(G_\infty, \mathcal{S}_p(E/F_\infty))$ is finite and satisfies

$$\sharp H^1(G_\infty, \mathcal{S}_p(E/F_\infty)) \,|\, \sharp\mathrm{Coker}(\varepsilon)\sharp H^3(G_\infty, E_{p^\infty}). \tag{36}$$

Since ψ_∞ is the composition of the map $X^{G_\infty} \hookrightarrow \left(\bigoplus_{v \in S} J_v(F_\infty)\right)^{G_\infty}$ and the map ε, it follows that $\sharp\mathrm{Coker}(\varepsilon) \,|\, \sharp\mathrm{Coker}(\psi_\infty)$. So we have the second part of Proposition 3.1. □

Remark. In fact, under certain conditions (in particular when $F = \boldsymbol{Q}$, discussed in [**24**]) it is possible to prove that ψ_∞ is a surjection, giving a stronger version of Propositions 3.1 and 3.3. This certainly fails for general fields F. We will not give details of this here but see [**15**] for a similar discussion in the cyclotomic $\boldsymbol{Z}_p$-extension case.

Recall the following sequence defining $\mathcal{S}_p(E/F_\infty)$:

$$0 \longrightarrow \mathcal{S}_p(E/F_\infty) \longrightarrow H^1(F^S/F_\infty, E_{p^\infty}) \xrightarrow{\lambda_{F_\infty}} \bigoplus_{v \in S} J_v(F_\infty) \tag{37}$$

Proposition 3.4. *For $p \geq 5$, the $\Lambda(R)$-rank of $\mathcal{C}_p(E/F_\infty)$ equals $|G_\infty : R|\tau_p(E/F)$ if and only if the map, λ_{F_∞}, in* (37) *is surjective.*

The basic idea here is to compute $\Lambda(R)$-ranks along the dual of the exact sequence, (37), above. We quote the following results from [**25**] and [**24**].

THEOREM 3.5. *The dual of* $H^1(F^S/F_\infty, E_{p^\infty})$ *has* $\Lambda(R)$*-rank equal to* $|F : \boldsymbol{Q}|\,|G_\infty : R|$, *independent of any conditions on* p.

THEOREM 3.6. *If* p *is any prime* ≥ 5, *then*

$$\bigoplus_{v \in S} \widehat{J_v(F_\infty)} \text{ has } \Lambda(R)\text{-rank equal to } |F : \boldsymbol{Q}|\,|G_\infty : R| - \tau_p(E/F) \tag{38}$$

The inequality of Theorem 2.5 mentioned above clearly follows from these.

PROOF OF PROPOSITION 3.4. The implication λ_{F_∞} surjective implies $\mathscr{C}_p(E/F_\infty)$ has the conjectured $\Lambda(R)$-rank is now clear from the determination of $\Lambda(R)$-ranks quoted. Conversely, suppose $\mathscr{C}_p(E/F_\infty)$ has the expected $\Lambda(R)$-rank. It follows from Theorems 3.5 and 3.6 that the dual of $\mathrm{Coker}(\lambda_{F_\infty})$ is $\Lambda(R)$-torsion. But the following argument, well known from the cyclotomic situation, shows that there is no non-zero $\Lambda(R)$-torsion in the dual of $\mathrm{Coker}(\lambda_{F_\infty})$, and hence it must be zero. Cassels' variant of the Poitou-Tate exact sequence extends (37) to

$$\begin{aligned} 0 \longrightarrow \mathscr{S}_p(E/F_\infty) \longrightarrow H^1(F^S/F_\infty, E_{p^\infty}) &\xrightarrow{\lambda_{F_\infty}} \bigoplus_{v \in S} J_v(F_\infty) \\ \longrightarrow \mathscr{R}_p(\widehat{E/F_\infty}) &\longrightarrow H^2(F^S/F_\infty, E_{p^\infty}), \end{aligned} \tag{39}$$

where $\mathscr{R}_p(E/F_\infty)$ is defined as the kernel of

$$\varprojlim H^1(F^S/F_n, F_{p^n}) \to \varprojlim \bigoplus_{\omega_n | S} H^1(F_{n,\omega_n}, E)(p^n). \tag{40}$$

Here, the limit is taken with respect to corestriction maps and the canonical maps induced by the multiplication by p maps, $\times p : E_{p^{n+1}} \to E_{p^n}$. Since $H^2(F^S/F_\infty, E_{p^\infty})$ is known to be zero from Theorem 2.10 above, it follows that the dual of $\mathrm{Coker}(\lambda_{F_\infty})$ is isomorphic to $\mathscr{R}_p(E/F_\infty)$. It is shown in [**25**], [**24**], however, that this is $\Lambda(R)$-torsion free. □

We shall see in §6 how Proposition 3.4 allows us to relate Conjecture 1.3 to the corresponding conjecture in the cyclotomic theory. Coping with potential supersingular primes is easier, though.

COROLLARY 3.7. *In particular,*

i) *if* $\mathscr{C}_p(E/F_\infty)$ *is* $\Lambda(R)$*-torsion, then* λ_{F_∞} *is a surjection,*

ii) *if* E *has potential supersingular reduction at all* v *dividing* p *then* $\tau_p(E/F) = |F : \boldsymbol{Q}|$ *and so, by Theorem* 2.5, *Conjecture* 2.4 *holds. It follows that for* $p \geq 5$ *the map* λ_{F_∞} *is a surjection.*

Assume until further notice that

HYPOTHESIS. i) $p \geq 5$
ii) *E has good, ordinary reduction at all primes of F dividing p*
iii) *$\mathcal{S}_p(E/F)$ is finite*
iv) *$\mathcal{C}_p(E/F_\infty)$ is $\Lambda(R)$-torsion*
That is, exactly the hypotheses of Theorem 1.1

PROOF OF THEOREM 1.1. Since the fourth hypothesis listed above forces the map λ_{F_∞} to be a surjection, taking G_∞ cohomology of (37) gives the following cohomological long exact sequence:

$$0 \longrightarrow \mathcal{S}_p(E/F_\infty)^{G_\infty} \longrightarrow H^1(F^S/F_\infty, E_{p^\infty})^{G_\infty} \xrightarrow{\psi_\infty}$$

$$\longrightarrow H^1(G_\infty, \mathcal{S}_p(E/F_\infty)) \longrightarrow \cdots \longrightarrow H^4\left(G_\infty, \bigoplus_{v \in S} J_v(F_\infty)\right) \longrightarrow 0 \quad (41)$$

The sequence terminating after the fourth cohomology groups because of the assumption that $p \geq 5$ and thus $\mathrm{cd}_p(G_\infty) = 4$. However, under the above hypotheses we can apply Proposition 3.3 to conclude that $\mathrm{Coker}(\psi_\infty)$ is finite. From Corollary 4.5 we have the isomorphisms

$$H^i(G_\infty, H^1(F^S/F_\infty, E_{p^\infty})) \cong H^{i+2}(G_\infty, E_{p^\infty}), \quad i \geq 1$$

and thus also the finiteness of these groups. Locally, by Lemma 5.16, we have the isomorphisms

$$H^i(G_\infty, J_v(F_\infty)) \cong H^{i+2}(\Delta_\omega, \tilde{E}_{v,p^\infty}) \quad \text{for } i \geq 1, \quad \text{any } v|p \text{ and any } \omega|v,$$

and these groups are again finite by Corollary 5.26. In fact, these groups are zero, but it is convenient to continue keeping track of them in the formulae for the present. Also, by Proposition 5.12,

$$H^i(G_\infty, J_v(F_\infty)) = 0 \quad \text{for } v \nmid p, \quad i \geq 1.$$

Thus all the terms appearing in (41) after $\mathrm{Coker}(\psi_\infty)$ are finite. In particular the groups $H^i(G_\infty, \mathcal{S}_p(E/F_\infty))$ for $i \geq 1$ are finite. But it was shown in Proposition 3.3 above that $H^0(G_\infty, \mathcal{S}_p(E/F_\infty))$ is finite, thus the Euler characteristic $\chi(G_\infty, \mathcal{S}_p(E/F_\infty))$ is defined. Taking the alternating product of the cardinalities of the terms in (41) appearing after the cokernel of ψ_∞ then gives the following formula

$$\sharp\mathrm{coker}(\psi_\infty) = \frac{\prod_{3 \leq i \leq 4} \sharp H^i(G_\infty, E_{p^\infty})^{(-1)^i}}{\prod_{1 \leq i \leq 4} \sharp H^i(G_\infty, \mathcal{S}_p(E/F_\infty)) \prod_{v|p} \left(\prod_{3 \leq i \leq 4} \sharp H^i(\Delta_\omega, \tilde{E}_{v,p^\infty})^{(-1)^i} \right)} \quad (42)$$

Substituting this into the formula given above (31), relating the cardinality of $\mathrm{coker}(\psi_\infty)$ with $\sharp(\mathcal{S}_p(E/F_\infty))^{G_\infty}$ we see that

$$\chi(G_\infty, \mathcal{S}_p(E/F_\infty)) = \frac{\rho_p(E/F)\left|\prod_{v\in\mathfrak{M}} L_v(E,1)\right|_p \chi(G_\infty, E_{p^\infty})}{\prod_{v|p}\chi(\Delta_\omega, \tilde{E}_{v,p^\infty})} \tag{43}$$

However, see Theorem 4.2 and Proposition 5.26 respectively, we know that for $v|p$

$$\chi(\Delta_\omega, \tilde{E}_{v,p^\infty}) = 1 = \chi(G_\infty, E_{p^\infty}),$$

thus completing the proof of Theorem 1.1. □

Now turn to the proof of Theorem 1.2. In fact, we can replace the hypotheses there by the following weaker hypotheses:

HYPOTHESIS. *Let G be any open subgroup of G_∞. Assume*
i) *G contains no element of order p*
ii) *The map λ_{F_∞} is surjective*

PROOF OF THEOREM 1.2. By replacing F by the fixed subfield of F we may assume $G = G_\infty$. Returning to the cohomological long exact sequence of (41), the conclusion of Theorem 1.2 follows immediately if we substitute in the facts: 1) that $H^i(G_\infty, H^1(F^S/F_\infty, E_{p^\infty})) = 0$ for $i \geq 2$ from Corollary 4.5 and 2) that $H^i(G_\infty, \bigoplus_{v\in S} J_v) = 0$ for $i \geq 1$ from Proposition 5.12 for v not dividing p and Lemma 5.16 together with Corollary 5.26 for v dividing p. This proves Theorem 1.2 as stated in the introduction because, by Corollary 3.7, the assumption that $\mathcal{C}_p(E/F_\infty)$ is $\Lambda(R)$-torsion implies that λ_{F_∞} is a surjection. □

We finish this section by proving the following result about the structure of $\mathcal{C}_p(E/F_\infty)$.

COROLLARY 3.8. *Under the hypotheses above for which we proved Theorem 1.2, $\mathcal{C}_p(E/F_\infty)$ contains no non-trivial, finite $\Lambda(\Omega)$-submodules, where Ω denotes any open subgroup of the Galois group,* $\mathrm{Gal}(F_\infty/F(\mu_{p^\infty}))$. *In particular, under these conditions the p-primary part of the Tate-Shafarevič group,* $Ш(E/F_\infty)(p)$, *is either infinite or zero.*

PROOF. Since Ω is an open subgroup of $\mathrm{Gal}(F_\infty/F(\mu_{p^\infty}))$ there exists some n sufficiently large such that $H_n = \mathrm{Gal}(F_\infty/F_n(\mu_{p^\infty}))$ is contained in Ω. Then it is sufficient to show there are no finite $\Lambda(H_n)$-submodules, where we consider $\mathcal{C}_p(E/F_\infty)$ as a $\Lambda(H_n)$-module in the only natural way, with the action induced by restricting that of G_∞. For n sufficiently large, H_n is a normal subgroup of

$\mathrm{Gal}(F_\infty/F_n)$ with quotient group, $\Gamma_n = \mathrm{Gal}(F_n(\mu_{p^\infty})/F_n)$, isomorphic to $\boldsymbol{Z}_p$ and having $cd_p(\Gamma_n) = 1$. The Hochschild-Serre spectral sequence thus gives rise to the exact sequence

$$0 \to H^1(\Gamma_n, H^2(H_n, \mathscr{S}_p(E/F_\infty))) \to H^3(\mathrm{Gal}(F_\infty/F_n), \mathscr{S}_p(E/F_\infty)) \to H^3(H_n, \mathscr{S}_p(E/F_\infty))^{\Gamma_n} \to 0. \tag{44}$$

But, under the above hypotheses, we know that $H^3(\mathrm{Gal}(F_\infty/F_n), \mathscr{S}_p(E/F_\infty)) = 0$. Thus the Γ_n-coinvariants of the discrete, p-primary $\Lambda(\Gamma_n)$-module $H^3(H_n, \mathscr{S}_p(E/F_\infty))$ vanish. Since Γ_n is pro-p, this implies the vanishing of $H^3(H_n, \mathscr{S}_p(E/F_\infty))$, by Nakayama's Lemma, 2.6. Suppose $M \subset \mathscr{C}_p(E/F_\infty)$ is a finite H_n-module. Then $\hat{M}$ is a finite quotient of $\mathscr{S}_p(E/F_\infty)$. Since we have $H^3(H_n, \mathscr{S}_p(E/F_\infty)) = 0$, $H^3(H_n, \hat{M}) = 0$. But since H_n is an open subgroup of $SL_2(\boldsymbol{Z}_p)$, H_n is an orientable Poincaré group of dimension equal to 3 and so $H^3(H_n, \hat{M})$ is dual to $H^0(H_n, M) = M^{H_n}$. Furthermore, this means $M^{H_n} = 0$. For H_n pro-p this is not possible by Nakayama's lemma, 2.6. The last comment follows because $Ш(E/F_\infty)(p)$ is the quotient of $\mathscr{S}_p(E/F_\infty)$ by $E(F_\infty) \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p$. □

REMARK. Corollary 3.8 is stronger than that showing $\mathscr{C}_p(E/F_\infty)$ contains no finite G-submodules for G any open subgroup of G_∞. This weaker statement follows in an identical manner only using the vanishing of $H^4(G, \mathscr{S}(E/F_\infty))$. One would expect the vanishing of $H^2(G, \mathscr{S}(E/F_\infty))$ should say something stronger yet about the structure of $\mathscr{C}_p(E/F_\infty)$, but it is not currently clear to us exactly what this could be.

Note in particular, it follows from Corollary 3.7 that both the vanishing of the higher cohomology and Corollary 3.8 hold for all $p \geq 5$ such that E has potential supersingular reduction at all primes of F dividing p.

4. Global Galois cohomology.

First we remark that the reduction type of E at p is clearly of no consequence for all the results in this section, and we make no assumption about it.

We require the following fact

LEMMA 4.1. *The cohomology groups, $H^i(G_\infty, E_{p^\infty})$ are finite for all p and all $i \geq 0$. They are zero for $i \geq 4$ if G_∞ contains no element of order p.*

This was first proved by Serre, [**37**] and [**40**], but is also easy to see in the following manner:

PROOF. Upon choosing a basis of T_pE, G_∞ is identified with an open subgroup of $GL_2(\boldsymbol{Z}_p)$. Then it contains a homothety, x, in the centre of G_∞ and acting upon E_{p^∞} as multiplication by $1 + p^t$ for some t. Because x lies in the

centre of G_∞ it acts trivially on the cohomology groups $H^i(G_\infty, E_{p^\infty})$. Thus $x-1$ annihilates the $H^i(G_\infty, E_{p^\infty})$. But $x-1$ also acts as multiplication by p^t, and so we have an exact sequence

$$0 \to H^i(G_\infty, E_{p^\infty}) \to H^{i+1}(G_\infty, E_{p^t}) \to H^{i+1}(G_\infty, E_{p^\infty}) \to 0 \tag{45}$$

for $i \geq 0$. Since all the $H^{i+1}(G_\infty, E_{p^t})$ are known to be finite (see [**28**] for the case when G_∞ is pro-p, but an elementary argument extends this to any p-adic Lie group) the finiteness part of the lemma follows. But if G_∞ has no elements of order p then we know it has p-cohomological dimension equal to 4, thus the vanishing for $i \geq 4$ follows from (45) in this case also. □

It follows that $\chi(G_\infty, E_{p^\infty})$ is defined when G_∞ contains no element of order p. In fact, in [**44**] Serre proved

THEOREM 4.2. *If G_∞ contains no element of order p then*

$$\chi(G_\infty, E_{p^\infty}) = 1 \tag{46}$$

As is shown in [**9**], Theorem 4.2 is in fact an easy consequence of the finiteness of the cohomology groups $H^i(\mathrm{Gal}(F_\infty/F^{cyc}), E_{p^\infty})$ for $i \geq 0$, where F^{cyc} denotes the cyclotomic $\boldsymbol{Z}_p$-extension of F. We shall use the finiteness of these cohomology groups in §6, and we are grateful to R. Sujatha for first pointing out their finiteness to us.

Let us quote the following result also needed, whose proof appears in [**8**]. For the remainder of this section we assume that p is odd.

LEMMA 4.3. *If $\mathcal{S}_p(E/F)$ is finite then $H^2(F^S/F, E_{p^\infty}) = 0$.*

We require one last fact.

LEMMA 4.4. *For all $i \geq 2$ we have*

$$H^i(G_\infty, H^1(F^S/F_\infty, E_{p^\infty})) = H^{i+2}(G_\infty, E_{p^\infty}) \tag{47}$$

If we also assume that $\mathcal{S}_p(E/F)$ is finite then (47) *holds for $i = 1$.*

COROLLARY 4.5. *Lemmas* 4.1 *and* 4.4 *together show that if G_∞ contains no element of order p then*

$$H^i(G_\infty, H^1(F^S/F_\infty, E_{p^\infty})) = 0 \quad \textit{for } i \geq 2. \tag{48}$$

If $\mathcal{S}_p(E/F)$ is also assumed to be finite then $H^1(G_\infty, H^1(F^S/F_\infty, E_{p^\infty}))$ is finite, of cardinality $\sharp H^3(G_\infty, E_{p^\infty})$,

We now give the proof of Lemma 4.4.

PROOF. Recall, from 2.10, that we know $H^2(F^S/F_\infty, E_{p^\infty}) = 0$. Thus the Serre-Hochschild sequence in group cohomology gives rise to the following exact sequence, for all $i \geq 2$,

$$\begin{aligned} &H^i(G_\infty, E_{p^\infty}) \to H^i(F^S/F, E_{p^\infty}) \to \\ &H^{i-1}(G_\infty, H^1(F^S/F, E_{p^\infty})) \to H^{i+1}(G_\infty, E_{p^\infty}) \to H^{i+1}(F^S/F, E_{p^\infty}). \end{aligned} \tag{49}$$

But it is well known that, since $p \neq 2$,

$$H^i(F^S/F, E_{p^\infty}) = 0 \quad \text{for } i \geq 3,$$

giving the first part of the lemma. If we make the additional hypothesis that $\mathcal{S}_p(E/F)$ is finite then the case $i = 2$ follows immediately from Lemma 4.3. □

We remark that it is certainly possible that $H^3(G_\infty, E_{p^\infty})$ be non-zero. Suppose $p \geq 5$ and so $\mathrm{cd}_p(G_\infty) = 4$. By the argument of the proof of Lemma 4.1 above, $H^3(G_\infty, E_{p^\infty}) \cong H^4(G_\infty, E_{p^t})$ for t sufficiently large. But it is known that G_∞ is a Poincaré group with dualising module $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. Thus $H^4(G_\infty, E_{p^t})$ has Poincaré dual $H^0(G_\infty, E_{p^t}(-1))$. This is non-zero if and only if E_{p^t} contains a submodule isomorphic to μ_p, the p^{th} roots of unity, as a G_∞-module. In particular, it is non-zero if both μ_p and a point of E_p are defined over F. We conclude this section with the following remark.

COROLLARY 4.6. *If Ω is any open subgroup of* $\mathrm{Gal}(F_\infty/F(\mu_{p^\infty}))$ *then the Pontrjagin dual of $H^1(F^S/F_\infty, E_{p^\infty})$ contains no finite, non-trivial, $\Lambda(\Omega)$-submodules.*

PROOF. Replacing F by F_n so as to ensure G_∞ contains no element of order p, this follows from Lemma 4.4 (the case $i = 3$) by an identical argument to the proof of Corollary 3.8. □

5. Local Galois cohomology.

We start by recalling our notation. Let v be any prime of F. Then ω denotes a prime of F_∞ dividing v. We denote by Δ_ω the decomposition group of ω in G_∞. Then the following explicit descriptions, as p-adic, Lie groups, of the Δ_ω are well known. See the appendix to chapter IV of Serre's book, [**39**].

LEMMA 5.1. i) *If v divides p then Δ_ω has dimension* 2 *if j_E is non-integral at v,* 3 *if E has potential ordinary reduction at v.*

ii) *If v does not divide p then the decomposition group, Δ_ω, has dimension* 2 *if j_E is non-integral at v, and dimension* 1 *otherwise.*

We sketch some of the ideas in this proof that will be needed later.

PROOF. Since the dimension is clearly invariant under finite extension of F_v we may as well replace F_v by a finite extension, L, and assume E has semistable reduction at v. Let $\Delta = \mathrm{Gal}(L_\infty/L)$ and let $L_\infty = L(E_{p^\infty})$.

We first dispose of the easy case when v does not divide p. But then if E has good reduction over L, by the results of Serre-Tate [**45**] L_∞/L is unramified and the group Δ is topologically generated by Frobenius, hence is one dimensional. If E has split multiplicative reduction then, by Tate's classification of such elliptic curves, we know that L_∞ is a Kummer extension, obtained by adjoining to $L(\mu_{p^\infty})$ the $p^{n^{\text{th}}}$ roots of the Tate period for all n. Thus it is clear that Δ has dimension 2.

We next turn to the case v divides p. Then the case of j_E non-integral exactly parallels the argument given above. Suppose now that E has good ordinary reduction over L, where the characteristic of the residue field of L is p. In this case it is most convenient to talk about the dimension of the corresponding Lie algebra, $\mathfrak{g} = \mathrm{Lie}(\Delta)$. Fix a minimal Weierstraß model for E defined over L, and let $\tilde{E}$ denote the reduced curve, defined over the residue field of L. Let $\hat{E}$ be the formal group over the integers, $\mathfrak{O}_L$, of L attached to the Néron model for E over $\mathfrak{O}_L$. We obtain an exact sequence of Galois modules

$$0 \to V_p(\hat{E}_{p^\infty}) \to V_pE \to V_p(\tilde{E}_{p^\infty}) \to 0 \tag{50}$$

where $V_p(\hat{E}_{p^\infty}) = T_p(\hat{E}_{p^\infty}) \otimes \boldsymbol{Q}_p$ is the $\boldsymbol{Q}_p$ vector space generated by the Tate module of the formal group and $V_p(\tilde{E}_{p^\infty})$ similarly is given by the Tate module of the points of p-power order on the reduced curve, $\tilde{E}$. Serre has shown (see [**39**]) that there exists a one dimensional subspace of V_pE which is a supplementary subspace of $V_p(\hat{E}_{p^\infty})$ and is stable under the action of $\mathfrak{g}$ *if and only if E has complex multiplication over L*. But our fundamental hypothesis throughout this paper is that E has no complex multiplication. Thus it follows (as in [**39**]) that $\mathfrak{g}$ is the Borel subalgebra of $End(V_pE)$ generated by the endomorphisms fixing the subspace $V_p(\hat{E}_{p^\infty})$ of V_pE. This is a 3-dimensional algebra. □

For future reference, we make the final step in the above proof more explicit. Choosing a basis of T_pE whose first element is a basis of $T_p(\hat{E}_{p^\infty})$ we have a faithful representation

$$\rho : \Delta \hookrightarrow GL_2(\boldsymbol{Z}_p); \quad \sigma \mapsto \begin{pmatrix} \psi(\sigma) & a(\sigma) \\ 0 & \phi(\sigma) \end{pmatrix} \tag{51}$$

where ψ is the character giving the action of Δ on $T_p(\hat{E}_{p^\infty})$, ϕ the character giving the action of Δ on $T_p(\tilde{E}_{p^\infty})$, and $a(\sigma) \in \boldsymbol{Z}_p$. The product $\psi\phi$ is the cyclotomic character, giving the action of Δ on μ_{p^∞}, by the Weil pairing. Then if H_∞ denotes the maximal unramified extension of L in L_∞, $\mathrm{Gal}(H_\infty/L)$ and $\mathrm{Gal}(H_\infty(\mu_{p^\infty})/H_\infty)$ are p-adic Lie groups of dimension 1 and $\sigma \mapsto a(\sigma)$ defines

an injection of $\mathrm{Gal}(L_\infty/H_\infty(\mu_{p^\infty}))$ into $\boldsymbol{Z}_p$. The point of Serre's theorem, as quoted above, is that since E has no complex multiplication the image of this map cannot be 0. Thus $\mathrm{Gal}(L_\infty/H_\infty(\mu_{p^\infty}))$ is isomorphic to $\boldsymbol{Z}_p$.

REMARK. Since it will not be necessary in any of the following arguments, we have not considered the case of potential supersingular reduction at all. This involves the concept of 'formal complex multiplication' of the p-divisible group, $\hat{E}_{p^\infty}$. See [**39**] for a description of $\mathfrak{g}$ in this case.

We now turn to the local cohomology calculations. Recall that, for any prime v of F, we defined

$$J_v(F_\infty) = \varinjlim \bigoplus_{\omega_n|v} H^1(F_{n,\omega_n}, E)(p) \tag{52}$$

We first study the G_∞-cohomology of this. Recall from 2.8 that this corresponds to studying the Δ_ω-cohomology of $H^1(F_{\infty,\omega}, E)(p)$ for any prime, ω, of F_∞ dividing v. We then turn to an analysis of the local restriction maps, δ_v, in diagram (16). As the methods involved are largely different we keep separate the cases where v divides p and where $v \nmid p$.

We start, however, with the following easy remarks which hold for all primes.

LEMMA 5.2. *For all $i \geq 1$ we have the isomorphism*

$$H^i(\Delta_\omega, H^1(F_{\infty,\omega}, E_{p^\infty})) \cong H^{i+2}(\Delta_\omega, E_{p^\infty}) \tag{53}$$

PROOF. We begin by observing that $H^2(L, E_{p^\infty}) = 0$ for each finite extension L of F_v. This is because Tate local duality shows that $H^2(L, E_{p^\infty})$ is dual to $H^0(L, T_pE)$, and this latter group is zero since the torsion subgroup of $E(L)$ is finite. Passing to the inductive limit over all finite extensions L of F_v contained in $F_{\infty,\omega}$, it follows that

$$H^2(F_{\infty,\omega}, E_{p^\infty}) = 0 \tag{54}$$

On the other hand, the absolute Galois group of $F_{\infty,\omega}$ has p-cohomological dimension at most 2 (see [**43**]) and so in fact

$$H^i(F_{\infty,\omega}, E_{p^\infty}) = 0, \quad \text{for all } i \geq 2. \tag{55}$$

But then the Hochschild-Serre spectral sequence [**23**] gives the exact sequence

$$H^{i+1}(F_v, E_{p^\infty}) \to H^i(\Delta_\omega, H^1(F_{\infty,\omega}, E_{p^\infty})) \to H^{i+2}(\Delta_\omega, E_{p^\infty}) \to H^{i+2}(F_v, E_{p^\infty}). \tag{56}$$

Since the first and last terms are zero for $i \geq 1$ the lemma follows. □

LEMMA 5.3. *The cohomology group* $H^2(F_{\infty,\omega}, E)(p)$ *equals zero and so, from the inflation restriction exact sequence* (19), $\mathrm{Coker}(\delta_v) = H^1(\Delta_v, E)(p)$.

PROOF. There is a canonical surjection

$$H^2(F_{\infty,\omega}, E_{p^\infty}) \to H^2(F_{\infty,\omega}, E)(p) \tag{57}$$

But the first group is zero from (54) above. □

5.1. Primes not dividing p.

We first dispose of this easier case. The reduction type of E at primes dividing p has no bearing here, and we make no hypothesis about this.

In this case, since v does not divide p, we have

$$E(L_\omega) \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p = 0 \tag{58}$$

for any algebraic extension, L of F, and any prime, ω of L, dividing v. In particular, it follows from Kummer theory that

$$H^1(F_v, E)(p) \cong H^1(F_v, E_{p^\infty}) \tag{59}$$

$$H^1(F_{\infty,\omega}, E)(p) \cong H^1(F_{\infty,\omega}, E_{p^\infty}) \tag{60}$$

LEMMA 5.4. *Suppose* $ord_v(j_E) < 0$. *Then* $J_v(F_\infty) = 0$.

PROOF. From (60) above, this will certainly follow if $\mathrm{Gal}(\overline{F_v}/F_{\infty,\omega})$ has p-cohomological dimension equal to zero. This, in turn, follows if we show $F_{\infty,\omega}$ contains the maximal pro-p extension of F_v. But this is clear. We know by the Weil pairing that $F_{\infty,\omega}$ contains the unique unramified $\boldsymbol{Z}_p$-extension of F_v as it contains $F_v(\mu_{p^\infty})$. Then it is well known (see [**42**]) that the maximal tamely ramified extension of F_v has a topologically cyclic Galois group over the maximal unramified extension. It follows that any Galois extension of $F_v(\mu_{p^\infty})$ whose profinite degree over $F_v(\mu_{p^\infty})$ is infinitely divisible by p must contain the maximal pro-p extension of F_v. But this holds for $F_{\infty,\omega}$, thanks to our hypothesis that $ord_v(j_E) < 0$, by Lemma 5.1. □

LEMMA 5.5. *Suppose* $ord_v(j_E) \geq 0$ *and* $p \geq 5$. *Then* $H^i(G_\infty, J_v(F_\infty)) = 0$ *for all* $i \geq 1$.

PROOF. Combining the isomorphisms (59, 60) with the Lemmas 2.8 and 5.2 the assertion of Lemma 5.5 is equivalent to showing that $H^i(\Delta_\omega, E_{p^\infty}) = 0$ for all $i \geq 3$. But Δ_ω has p-cohomological dimension equal to 1 in this case. This is because it has dimension 1 as a p-adic Lie group, from Lemma 5.1. Since it is a closed subgroup of G_∞ and so the hypothesis that $p \geq 5$ ensures Δ_ω contains no element of order p, $cd_p(\Delta_\omega)$ equals 1 by Theorem 2.2. □

REMARK. The assumption that $p \geq 5$ is only required in case E has unstable reduction at v. If E has good reduction then the extension $F_{\infty,\omega}/F_v$ is unramified. Since it contains the maximal unramified pro-p extension, Δ_ω has p-cohomological dimension equal to 1 for any choice of p.

We now carry out the crucial analysis of the kernel and cokernel of the local restriction maps

$$\delta_v : H^1(F_v, E)(p) \to (J_v(F_\infty))^{G_\infty} \cong H^1(F_{\infty,\omega}, E)(p)^{\Delta_\omega} \tag{61}$$

postponed from the proof of Theorem 1.1. In the light of the isomorphisms (59, 60) in this case (of $v \not| p$) we may replace (61) by an analysis of

$$\delta_v : H^1(F_v, E_{p^\infty}) \to H^1(F_{\infty,\omega}, E_{p^\infty})^{\Delta_\omega} \tag{62}$$

Then the inflation restriction sequence (19) describing the kernel and cokernel of δ_v becomes in this case

$$\begin{aligned} 0 \to H^1(\Delta_\omega, E_{p^\infty}) \to H^1(F_v, E_{p^\infty}) &\xrightarrow{\delta_v} H^1(F_{\infty,\omega}, E_{p^\infty})^{\Delta_\omega} \\ &\to H^2(\Delta_\omega, E_{p^\infty}) \to 0 \end{aligned} \tag{63}$$

where the 0 on the right is because $H^2(F_v, E_{p^\infty}) = 0$ by (54).

Recall that $c_v = |E(F_v) : E_0(F_v)|$, the local Tamagawa factor, and $L_v(E, s)$ denotes the Euler factor of the complex L-function of E at v. We quote the following well known lemma (see [**8**]).

LEMMA 5.6. *Let v be any finite prime of F not dividing p. Then $H^1(F_v, E)(p)$ is finite, of order the exact power of p dividing $c_v/L_v(E, 1)$.*

We will omit the proof here.

REMARK. We now see the reason for the appearance of the Euler factors in Theorem 1.1. For any number field H, we define a *restricted Selmer group* by

$$\mathcal{S}_p'(E/H) = \mathrm{Ker}\left(H^1(H^S/H, E_{p^\infty}) \to \bigoplus_{v \in S \setminus \mathfrak{M}} H^1(H_v, E)(p) \right) \tag{64}$$

where S and $\mathfrak{M}$ are the sets of primes of H defined as always. Then Lemma 5.4 states that $\mathcal{S}_p'(E/F_\infty) = \varinjlim \mathcal{S}_p'(E/F_n)$ satisfies

$$\mathcal{S}_p'(E/F_\infty) = \mathcal{S}_p(E/F_\infty) \tag{65}$$

As always, let F^{cyc} denote the cyclotomic $\boldsymbol{Z}_p$-extension of F. Then it is generally not true that $\mathcal{S}_p'(E/F^{cyc}) = \mathcal{S}_p(E/F^{cyc})$. If Γ denotes the Galois group of F^{cyc} over F then, as we remarked above, it is well known that

THEOREM 5.7 (Perrin-Riou, Schneider). *Under the conditions* (i), (ii) *and* (iii) *of Theorem* 1.1, $\mathcal{S}_p(\widehat{E/F^{cyc}})$ *is* $\Lambda(\Gamma)$*-torsion and*

$$\chi(\Gamma, \mathcal{S}_p(E/F^{cyc})) = \rho_p(E/F). \tag{66}$$

If one instead considers the restricted Selmer group then the following variant of this theorem is easy to check (see [**24**]).

If M is a discrete p-primary Γ-module such that its Pontrjagin dual $\hat{M}$ is a finitely generated, torsion $\Lambda(\Gamma)$-module, we write $char(M)$ for the characteristic ideal of $\hat{M}$.

COROLLARY 5.8. *Under conditions* (i), (ii) *and* (iii) *of Theorem* 1.1 *the restricted Selmer group,* $\mathcal{S}_p'(\widehat{E/F_\infty^{cyc}})$, *is* $\Lambda(\Gamma)$*-torsion. Then*

$$char(\mathcal{S}_p'(E/F_\infty^{cyc})) = char(\mathcal{S}_p(E/F_\infty^{cyc})) \times char\left(\bigoplus_{v \in \mathfrak{M}} H^1(F_v^{cyc}, E)(p)\right). \tag{67}$$

The characteristic power series of the dual of $\bigoplus_{v \in \mathfrak{M}} H^1(F_v^{cyc}, E)(p)$ *does not vanish at* $T = 0$, *and its value there is equal, up to a p-adic unit, to*

$$\left| \prod_{v \in \mathfrak{M}} L_v(E, 1) \right|_p .$$

Thus

$$\chi(\Gamma, \mathcal{S}_p'(E/F^{cyc})) = \rho_p(E/F) \times \left| \prod_{v \in \mathfrak{M}} L_v(E, 1) \right|_p \tag{68}$$

We note that $\bigoplus_{v \in \mathfrak{M}} H^1(F_v^{cyc}, E)(p)$ is known to be $\Lambda(\Gamma)$-cotorsion by results of Greenberg's in [**16**]. Thus Conjecture 1.4 can be interpreted as saying that under the given conditions on E and p

$$\chi(G_\infty, \mathcal{S}_p'(E/F_\infty)) = \chi(\Gamma, \mathcal{S}_p'(E/F^{cyc})), \tag{69}$$

illustrating further the analogy between this new situation and the classical choice of the cyclotomic $\boldsymbol{Z}_p$-extension.

LEMMA 5.9. *For* $p \geq 5$ *and for primes* v *not dividing* p *the map* δ_v *is a surjection and thus* $H^2(\Delta_\omega, E_{p^\infty}) = 0$.

PROOF. If $ord_v(j_E) < 0$ then this is immediate because $H^1(F_{\infty,\omega}, E_{p^\infty})$ equals zero from Lemma 5.4. So suppose $ord_v(j_E) \geq 0$. Now we need the hypothesis that $p \geq 5$. But in this case we know that Δ_ω has p-cohomological dimension equal to 1, as in the proof of Lemma 5.5. □

LEMMA 5.10. *For primes v not dividing p, if $ord_v(j_E) \geq 0$ and $p \geq 5$, then δ_v is an injection.*

PROOF. Recall F_v^{cyc} denotes the cyclotomic $\boldsymbol{Z}_p$-extension of F_v and Γ the Galois group $\mathrm{Gal}(F_v^{cyc}/F_v)$. Let $\Phi = \mathrm{Gal}(F_{\infty,\omega}/F_v^{cyc})$. Then we have exact sequence

$$0 \to H^1(\Gamma, E_{p^\infty}(F_v^{cyc})) \to \mathrm{Ker}(\delta_v) \to H^1(\Phi, E_{p^\infty})^\Gamma \tag{70}$$

Now both $F_{\infty,\omega}$ and F_v^{cyc} contain the unramified $\boldsymbol{Z}_p$-extension of F_v and, as in the proof of 5.1, the results of Serre-Tate [**45**] show that the order of the inertial subgroup of Δ_ω is prime to p. Thus Φ has profinite (in fact, finite) degree prime to p and so the final term in (70) is 0. The lemma will follow from the following well known result in the cyclotomic theory, which we quote without proof. □

LEMMA 5.11. *Let v be any finite prime of F not dividing p. As above, let F_v^{cyc} denote the cyclotomic $\boldsymbol{Z}_p$-extension of F_v and set $\Gamma = \mathrm{Gal}(F_v^{cyc}/F_v)$. Then $H^1(\Gamma, E_{p^\infty}(F_v^{cyc}))$ is finite, of order the exact power of p dividing $c_v = |E(F_v) : E_0(F_v)|$.*

REMARK. In this case of $ord_v(j_E) \geq 0$ and $p \geq 5$ the maximal power of p dividing c_v is 1 because it is well known that the only primes dividing c_v lie in $\{2, 3\}$. Thus it is convenient to say that

$$\sharp\mathrm{Ker}(\delta_v) = |c_v|_p^{-1} \tag{71}$$

and to include c_v in the definition of $\rho_p(E/F)$ in (7) above. In fact, we will see later that an analysis of the case $p = 3$ indicates this is the correct formulation. For $p = 3$ the map δ_v can fail to be an injection and then $\mathrm{Ker}(\delta_v) = |c_v|_p^{-1}$. Also, if E has additive reduction then $L_v(E, 1) = 1$ and so we could include this factor and enlarge the set $\mathfrak{M}$ in the statement of Theorem 1.1. We do not do this however.

We remark again that the hypothesis $p \geq 5$ is only required to deal with the case where E has additive reduction at v.

For convenience, we here gather together the results proven above at primes of F not dividing p.

PROPOSITION 5.12. *Assume v does not divide p. Then*

i) $H^i(G_\infty, J_v(F_\infty)) \cong H^{i+2}(\Delta_\omega, E_{p^\infty})$, for all $i \geq 1$.

ii) *If $ord_v(j_E) < 0$ then $J_v(F_\infty) = 0$. Hence $\mathrm{Coker}(\delta_v) = 0$, and also*

$$\sharp\mathrm{Ker}(\delta_v) = \left|\frac{L_v(E, 1)}{c_v}\right|_p.$$

iii) *If* $ord_v(j_E) \geq 0$ *and* $p \geq 5$ *then*

$$H^j(\Delta_\omega, E_{p^\infty}) = 0, \quad \text{for } j \geq 1$$

and so δ_v *is an isomorphism.*

iv) *If* E *has good reduction at* v *then we can remove the condition* $p \geq 5$ *above.*

We take the opportunity here to give the following lemma, which will be of use later.

LEMMA 5.13. *Let* K *be a finite extension of* $\boldsymbol{Q}_q$ *for* q *a rational prime with* $(q, p) = 1$. *Let* E *be an elliptic curve defined over* K *such that* E *has potential multiplicative reduction over* K. *Let* $K_\infty = K(E_{p^\infty})$ *and let* $\Omega = \mathrm{Gal}(K_\infty/K(\mu_{p^\infty}))$.

i) *If* E *has split multiplicative reduction over* $K(\mu_p)$ *then*

$$H^1(\Omega, E(K_\infty))(p) = \boldsymbol{Q}_p/\boldsymbol{Z}_p. \tag{72}$$

ii) *Assume* $p > 2$. *If* E *has potential, but not split, multiplicative reduction over* $K(\mu_p)$ *then*

$$H^1(\Omega, E(K_\infty))(p) = 0. \tag{73}$$

PROOF. Since K is assumed to have residue characteristic different from p, it follows from Kummer theory that

$$H^1(\Omega, E(K_\infty))(p) = H^1(\Omega, E_{p^\infty}) \tag{74}$$

as in (59) and (60).

i) By the Tate parameterisation, E_{p^∞} fits into the canonical short exact sequence of $G_{K(\mu_p)}$-modules

$$0 \to \mu_{p^\infty} \to E_{p^\infty} \to \boldsymbol{Q}_p/\boldsymbol{Z}_p \to 0, \tag{75}$$

which does not split. But, as there is split multiplicative reduction over $K(\mu_p)$, K_∞ is obtained by adjoining to $K(\mu_{p^\infty})$ all the p^{th}-power roots of the Tate period, q_E, of E and so $\Omega \cong \boldsymbol{Z}_p$ as an Abelian group. Also, Ω acts trivially upon the first and third terms in (75). Taking Ω cohomology, we obtain

$$0 \to \boldsymbol{Q}_p/\boldsymbol{Z}_p \to H^1(\Omega, \mu_{p^\infty}) \to H^1(\Omega, E_{p^\infty}) \to H^1(\Omega, \boldsymbol{Q}_p/\boldsymbol{Z}_p) \to 0 \tag{76}$$

where $H^1(\Omega, \mu_{p^\infty}) \cong H^1(\Omega, \boldsymbol{Q}_p/\boldsymbol{Z}_p) \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p$, from which (72) follows.

ii) Assume E has potential (but not split) multiplicative reduction over $K(\mu_p)$. Let K' be a quadratic extension of $K(\mu_p)$ over which E achieves split multiplicative reduction. Set $K'_\infty = K'(E_{p^\infty})$ and let $\Omega' = \mathrm{Gal}(K'_\infty/K'(\mu_{p^\infty}))$.

Let $\Delta = \mathrm{Gal}(K'/K(\mu_p))$. It follows from the assumption that $p > 2$ that E does not attain split multiplicative reduction over $K(\mu_{p^\infty})$ and so if Δ' denotes $\mathrm{Gal}(K'(\mu_{p^\infty})/K(\mu_{p^\infty}))$ then Δ' has order 2. Then, again using that $p > 2$, it follows from the Hochschild-Serre spectral sequence that

$$H^1(\Omega, E_{p^\infty}) = H^1(\Omega', E_{p^\infty})^{\Delta'} \tag{77}$$

But from the first case we know that

$$H^1(\Omega', E_{p^\infty}) \cong H^1(\Omega', D) \tag{78}$$

where $D \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p$ as an Ω'-module but Δ' acts on D via its non-trivial character. Again, $\Omega' \cong \boldsymbol{Z}_p$ as an Abelian group. One sees that the action of Δ' on Ω', by conjugation, is trivial because the Tate period q_E is defined over K. Thus the action of Δ' on

$$H^1(\Omega', D) \cong \mathrm{Hom}(\Omega', D) \tag{79}$$

is via its non-trivial character, and so

$$H^1(\Omega', D)^{\Delta'} = 0 \tag{80}$$

□

We conclude this subsection by giving a brief description of what happens when $p = 3$. These remarks are not required anywhere else in this paper since we assume p to be at least 5 for all the main results. We include them only to explain what might otherwise appear to be a curious choice in the formulation of Theorem 1.1. There we include the Tamagawa factors, c_v, in the formula (7) for $\rho_p(E/F)$ for all places v of F at which E has bad reduction. It follows from our restriction to $p \geq 5$ that $|c_v|_p = 1$ for all places v at which j_E is integral and thus it might appear more natural to include only the terms coming from the Tamagawa factors at places where j_E is non-integral. The following description of the behaviour when $p = 3$ motivates our choice to retain these extra terms. As noted above in the statement of Proposition 5.12, taking p to equal 3 only causes difficulties for primes $v \not| 3$ such that E has bad reduction but $ord_v(j_E) \geq 0$. Then E has additive reduction at v and $L_v(E, 1) = 1$. Assume v is such a prime of F for the remainder of this subsection.

Lemma 5.14. i) *The* $H^i(\Delta_\omega, E_{3^\infty})$ *are finite for all* $i \geq 0$ *and satisfy*

$$\sharp H^i(\Delta_\omega, E_{3^\infty}) = \sharp H^{i+2}(\Delta_\omega, E_{3^\infty}) \tag{81}$$

It is possible for both to be non-zero.

ii) *The cardinality of* $\mathrm{Ker}(\delta_v)$ *is given by* $\sharp H^1(\Delta_\omega, E_{3^\infty}) = |c_v|_3^{-1}$.

The significant point for our choice of the formulation of Theorem 1.1 is part (ii) which follows from the exact sequence (70) together with Lemmas 5.6 and 5.11. For (i) we content ourselves with remarking that it involves explicit calculations for $\mathrm{Gal}(F_v(E_3)/F_v)$ isomorphic to each possible subgroup of $GL_2(\boldsymbol{F}_3)$, using the classification of such subgroups (as described in, for example, [**41**].) We will not give the proof as it is lengthy and not especially enlightening. Some details are in [**24**].

It follows from Lemma 5.14 that $\chi(G_\infty, \mathcal{S}_p(E/F_\infty))$ may fail to be defined for $p = 3$.

5.2. Primes dividing p.

We now consider results analogous to 5.12 above, but for primes of F dividing p. This situation is more subtle (and in fact we cannot obtain quite such a complete result) for two reasons. The first is that Δ_ω will generally have higher p-cohomological dimension. It can, in fact, have p-cohomological dimension 4 at potential supersingular primes, but this case will not concern us. Secondly, and more seriously, there are no longer simple isomorphisms like those of (59, 60) describing the image of Kummer in terms of an appropriate discrete, p-primary, Galois module. Fortunately, however, the ramification theoretic methods developed by one of us in joint work with R. Greenberg (see [**5**]) provide a solution to this problem. We also note that our treatment of the possibility that E has unstable reduction at v has been inspired by the methods used by D. Delbourgo in [**12**] for the cyclotomic $\boldsymbol{Z}_p$-extension.

Throughout this subsection v will denote an arbitrary prime of F dividing p, ω a prime of F_∞ above v. We will omit this hypothesis from the statement of all the results. Write G_v for the Galois group of $\overline{F_v}$ over F_v and I_v for the inertial subgroup of G_v. As explained in [**5**], it is easy to see that there is a canonical exact sequence of G_v-modules

$$0 \to C \to E_{p^\infty} \to D \to 0 \tag{82}$$

characterised by the fact that C is divisible and D is the maximal quotient of E_{p^∞} by a divisible subgroup such that I_v acts on D via a finite quotient. In particular, D is zero if and only if E has potential supersingular reduction at v. If E has good ordinary reduction at v then D can be identified with $\tilde{E}_{v,p^\infty}$, the p-primary subgroup of $\tilde{E}_v$. Recall, $\tilde{E}_v$ denotes the reduction of E modulo v.

We note that $F_{\infty,\omega}$ is deeply ramified in the sense of [**5**], because it contains the subextension $F_v(\mu_{p^\infty})$ which is itself already deeply ramified.Hence we can apply the results of that paper to give the required description of the image of the Kummer map.

PROPOSITION 5.15. (Propositions 4.3 and 4.8 of [5]).

$$H^1(F_{\infty,\omega}, E)(p) \cong H^1(F_{\infty,\omega}, D) \tag{83}$$

We prove the following analogue of Lemma 5.2 without any assumption on the reduction type of E at v.

LEMMA 5.16. *For all* $i \geq 1$

$$H^i(G_\infty, J_v(F_\infty)) \cong H^{i+2}(\Delta_\omega, D), \tag{84}$$

where D *is defined by* (83) *above.*

PROOF. We note that $\mathrm{Gal}(\overline{F_v}/F_{\infty,\omega})$ has p-cohomological dimension less than or equal to 1 because the profinite degree of $F_{\infty,\omega}$ over F_v is divisible by p^∞ (see [**43**]). It follows that

$$H^i(F_{\infty,\omega}, D) = 0, \quad \text{for } i \geq 2. \tag{85}$$

Thus, as in the proof of 5.2, the Hochschild-Serre spectral sequence applied to the extension $F_{\infty,\omega}$ over F_v gives exact sequences

$$H^{i+1}(F_v, D) \to H^i(\Delta_\omega, H^1(F_{\infty,\omega}, D)) \to H^{i+2}(\Delta_\omega, D) \to H^{i+2}(F_v, D) \tag{86}$$

for $i \geq 1$. Since G_v has p-cohomological dimension equal to 2 the lemma follows from this sequence (together with 2.8) for $i \geq 2$. It remains to show $H^2(F_v, D) = 0$. But $H^2(F_v, E_{p^\infty}) = 0$ as in the proof of Lemma 5.2 and $H^3(F_v, C) = 0$ by cohomological dimension. Taking G_v-cohomology of (82), we see that $H^2(F_v, D) = 0$ also. □

We will turn to a more explicit description of the $H^i(\Delta_\omega, D)$ later. First we give an analysis of the local restriction maps, δ_v, reducing this question also to a description of some $H^i(\Delta_\omega, D)$. In the case $v|p$, Tate local duality shows that $H^1(F_v, E)(p)$ is dual to

$$E(F_v)\hat{\otimes}\boldsymbol{Z}_p \cong \boldsymbol{Z}_p^d \times E(F_v)(p) \tag{87}$$

where $d = |F_v : \boldsymbol{Q}_p|$. In particular, $H^1(F_v, E)(p)$ is always infinite (in contrast to the case of $v \nmid p$, Lemma 5.6)

LEMMA 5.17. *Assume that* E *has potential supersingular reduction at* v. *Then* δ_v *is the zero map. Hence in particular* $\mathrm{Ker}(\delta_v)$ *is infinite. We also have* $\mathrm{Coker}(\delta_v)$ *is zero.*

PROOF. This follows trivially from the remark made above that D is zero if and only if E has potential supersingular reduction at v. The group $J_v(F_\infty)$ is contained in $\prod_\omega H^1(F_{\infty,\omega}, E)(p)$, which is now zero by Proposition 5.15. □

As we remarked above, when E has potential multiplicative reduction at a prime of F dividing p it is conjectured that $\mathrm{Ker}(\delta_v)$ is finite, but is generally unknown. The only case which is known is $F = \boldsymbol{Q}$, the proof of which depends upon a transcendence result of [**2**]. We will need to say something about this case in order to prove Theorem 1.5. We start, however, with the case $ord_v(j_E) \geq 0$.

HYPOTHESIS (PG). i) $p \geq 5$, ii) $ord_v(j_E) \geq 0$.

By Corollary 2 of Theorem 2 of Serre-Tate [**45**], Hypothesis (PG) implies that there exists a finite extension, K of F_v, satisfying

i) *E has good ordinary reduction over K*

ii) *K is a Galois extension of F_v*

iii) *$|K : F_v|$ is prime to p.*

It follows immediately that $K_\infty = K(E_{p^\infty})$ is also a Galois extension of $F_{\infty,\omega}$ of finite degree prime to p. For example, [**45**] shows that one could take $K = F_v(E_3)$ which is a Galois extension of F_v of degree dividing 48. We fix any such choice of K whenever (PG), or the following, stronger Hypotheses (PO), is assumed to hold.

HYPOTHESIS (PO). i) $p \geq 5$, ii) *E has potential ordinary reduction at v.*

Let $\hat{E}$ denote the formal group of E defined over K. As explained in [**5**] page 151, we can take the p-divisible group C appearing in (82) to be the Galois module consisting of the torsion points in $\hat{E}(\bar{\mathscr{M}})$, denoted $\hat{E}(\bar{\mathscr{M}})_{p^\infty}$. Here, $\bar{\mathscr{M}}$ is the maximal ideal of the ring of integers of $\overline{F_v}$. We have the exact sequence

$$0 \to \hat{E}(\mathscr{M}(K_\infty)) \to E(K_\infty) \to \tilde{E}(k_{K_\infty}) \to 0 \tag{88}$$

where $\mathscr{M}(K_\infty)$ denotes the maximal ideal of the ring of integers of K_∞, and $\tilde{E}$ the reduction of E over K.

Let $\Theta = \mathrm{Gal}(K_\infty/F_v)$, $H = \mathrm{Gal}(K_\infty/F_{\infty,\omega})$ and $T = \mathrm{Gal}(K/F_v)$. It is clear from the sequence (83) and the identification of C with $\hat{E}(\bar{\mathscr{M}})_{p^\infty}$ that D can be identified with $\tilde{E}(k_{K_\infty})_{p^\infty}$. Let $\mathfrak{F}$ denote the reduction map

$$\mathfrak{F} : E(K) \to \tilde{E}(k_K). \tag{89}$$

Restricting to the subset $E(F_v)$ of $E(K)$ gives a map, also denoted by $\mathfrak{F}$,

$$\mathfrak{F} : E(F_v) \to \tilde{E}(k_K)^T \tag{90}$$

LEMMA 5.18. *Assume Hypothesis* (PG). *Then*

i) *for $i \geq 2$ we have the isomorphism*

$$H^i(\Delta_\omega, E(F_{\infty,\omega}))(p) \cong H^i(\Theta, D). \tag{91}$$

ii) *The following is exact.*

$$0 \to \frac{\tilde{E}(k_K)^T(p)}{\mathfrak{F}(E(F_v))(p)} \to H^1(F_v, \hat{E}(\bar{\mathscr{M}}))(p) \to H^1(\Delta_\omega, E(F_{\infty,\omega}))(p)$$
$$\to H^1(\Theta, D) \to 0 \tag{92}$$

PROOF. As remarked earlier $F_{\infty,\omega}$, and thus also K_∞, is deeply ramified. It follows from the principal result of [**5**] that

$$H^i(K_\infty, \hat{E}(\bar{\mathscr{M}})) = 0, \quad \text{for } i \geq 1. \tag{93}$$

By the Hochschild-Serre spectral sequence, this vanishing implies

$$H^i(\Theta, \hat{E}(\mathscr{M}(K_\infty))) \cong H^i(F_v, \hat{E}(\bar{\mathscr{M}})), \quad \text{for } i \geq 1. \tag{94}$$

We first show

$$H^i(F_v, \hat{E}(\bar{\mathscr{M}})) = 0, \quad \text{for } i \geq 2. \tag{95}$$

But by Kummer theory we have a surjection

$$H^i(F_v, C) \twoheadrightarrow H^i(F_v, \hat{E}(\bar{\mathscr{M}}))(p), \quad \text{for all } i, \tag{96}$$

using the identification of C with $\hat{E}(\bar{\mathscr{M}})_{p^\infty}$. Hence it is sufficient to show $H^i(F_v, C) = 0$ for $i \geq 2$. This is clear for $i \geq 3$ by the fact that the cohomological dimension of G_v equals 2. For $i = 2$, if E has potential supersingular reduction over F_v then $C = E_{p^\infty}$ and so this follows from (54) appearing in the proof of Lemma 5.2 above. Finally, if E has potential ordinary reduction over F_v then C has $\boldsymbol{Z}_p$-corank equal to 1 and is its own orthogonal complement under the Weil pairing. Thus $H^2(F_v, C)$ is dual to $H^0(F_v, T_pD)$. Since only finitely many points of $\tilde{E}(k_K)_{p^\infty}$ are rational over k_K it follows that $H^0(K, T_pD)$ equals zero and thus so also is $H^0(F_v, T_pD)$. We now take Θ-cohomology of the exact sequence (88). By (94) and (95) this gives an isomorphism

$$H^i(\Theta, E(K_\infty))(p) \xrightarrow{\sim} H^i(\Theta, \tilde{E}(k_{K_\infty}))(p), \quad \text{for } i \geq 2. \tag{97}$$

Since $\tilde{E}(k_{K_\infty})$ is torsion, the right hand side may be identified with $H^i(\Theta, \tilde{E}(k_{K_\infty})_{p^\infty})$. Now Δ_ω is the quotient of Θ by H, a finite group of order prime to p. It follows from the Hochschild-Serre spectral sequence that the inflation map gives an isomorphism

$$H^i(\Delta_\omega, E(F_{\infty,\omega}))(p) \xrightarrow{\sim} H^i(\Theta, E(K_\infty))(p), \quad \text{for all } i. \tag{98}$$

On identifying $\tilde{E}(k_{K_\infty})_{p^\infty}$ with D, we obtain the first part of the lemma. Substituting what we have discovered so far into the long exact sequence of

cohomology obtained on taking Θ-cohomology of (88) gives the exact sequence in part (ii) immediately. □

The first thing to observe is that $\tilde{E}(k_K)(p)$ is finite and thus so is the first term in (92). We next turn our attention to the second term.

LEMMA 5.19. *Assume Hypothesis* (PG) *The group* $H^1(F_v, \hat{E}(\bar{\mathcal{M}}))(p)$ *is finite if and only if* E *has potential ordinary reduction over* F_v. *In this case,* $H^1(F_v, \hat{E}(\bar{\mathcal{M}}))(p)$ *is cyclic, dual to* $\tilde{E}(k_K)^T(p)$.

PROOF. We could deduce the only if part of this from 5.17. However, we shall proceed independently. We have the exact sequence

$$0 \to \hat{E}(\mathcal{M}(F_v)) \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p \to H^1(F_v, C) \to H^1(F_v, \hat{E}(\bar{\mathcal{M}}))(p) \to 0 \qquad (99)$$

All three terms in (99) are cofinitely generated as $\boldsymbol{Z}_p$-modules. Let h_v be the height of the formal group $\hat{E}$, thus h_v equals 1 or 2 according as E has potential good ordinary or potential good supersingular reduction at v. The elementary theory of the formal group tells us that the group on the left of (99) is divisible of $\boldsymbol{Z}_p$-corank equal to $d_v = |F_v : \boldsymbol{Q}_p|$. It follows easily from Tate's local Euler characteristic theorem (described, for example, in [**31**]) that the dual of $H^1(F_v, C)$ is a finitely generated $\boldsymbol{Z}_p$-module of $\boldsymbol{Z}_p$-rank equal to $d_v h_v$. Thus the group on the right is finite if and only if $h_v = 1$. Suppose this is the case. For convenience let W denote $H^1(F_v, C)$ and W_{div} the maximal divisible subgroup of W. Then we have just seen that in this case

$$W_{div} = \hat{E}(\mathcal{M}(F_v)) \otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

with $W/W_{div} = H^1(F_v, \hat{E}(\bar{\mathcal{M}}))(p)$ finite. We introduce the $\boldsymbol{Q}_p$-vector space $V_p(\hat{E}) \cong T_p(\hat{E}) \otimes_{\boldsymbol{Z}_p} \boldsymbol{Q}_p$ as in the proof of 5.1. Then the continuous cohomology groups $H^i(F_v, V_p(\hat{E}))$ are also $\boldsymbol{Q}_p$ vector spaces and so, in particular, are divisible for all i. The continuous cohomology groups, $H^i(F_v, T_p(\hat{E}))$, however are finitely generated as $\boldsymbol{Z}_p$-modules. Taking cohomology of the exact sequence

$$0 \to T_p(\hat{E}) \to V_p(\hat{E}) \to C \to 0 \qquad (100)$$

we deduce from the above remarks that there is an isomorphism

$$W/W_{div} \cong H^2(F_v, T_p(\hat{E}))$$

Since we are now assuming that h_v equals 1, the p-divisible group C has $\boldsymbol{Z}_p$-corank equal to 1 and is its own orthogonal complement under the Weil pairing. It follows from Tate local duality that $H^2(F_v, T_p(\hat{E}))$ is dual to $H^0(F_v, D)$. This latter group is exactly as claimed in the lemma. □

In fact we at no point required that $|K : F_v|$ be prime to p for the proof of Lemma 5.19 which thus also holds for $p = 2, 3$.

We restrict now to the potential ordinary case.

COROLLARY 5.20. *Assume Hypothesis* (PO). *Then there is an exact sequence*

$$0 \to \frac{\tilde{E}(k_K)^T(p)}{\mathfrak{F}(E(F_v))(p)} \to \widehat{\tilde{E}(k_K)^T}(p) \to H^1(\Delta_\omega, E(F_{\infty,\omega}))(p) \tag{101}$$

and thus, as an Abelian group, $H^1(\Delta_\omega, E(F_{\infty,\omega}))(p)$ *contains a finite cyclic subgroup isomorphic to* $\mathfrak{F}(E(F_v))(p)$.

LEMMA 5.21. *Assume Hypothesis* (PO). *Then we have isomorphisms*

$$H^i(\Delta_\omega, D) \cong H^i(\Theta, D) \tag{102}$$

for all $i \geq 0$. *These groups are finite, and are zero for* $i \geq 3$.

PROOF. The isomorphism (102) follows exactly as in the proof of Lemma 5.18, from the Hochschild-Serre spectral sequence. (Recall Δ_ω is the quotient of Θ by a finite subgroup of order prime to p and D is p-primary.) Let $\Omega = \mathrm{Gal}(K_\infty/K)$, a subgroup of Θ of finite index, prime to p. Then, again by the Hochschild-Serre spectral sequence, it is sufficient to prove the $H^i(\Omega, D)$ are finite for all i and equal to zero for $i \geq 3$. But now E has good ordinary reduction over K and D is simply $\tilde{E}(k_K)_{p^\infty}$. Then Ω embeds, as an open subgroup, into the subgroup of $GL_2(\boldsymbol{Z}_p)$ consisting of the upper triangular matrices, as in (51). The finiteness of the $H^i(\Omega, D)$ and vanishing for $i \geq 3$ now follows by an identical argument to the proof of Lemma 4.1 in the previous section. We see from (51) that Ω has p-cohomological dimension equal to 3 and contains a central element which acts on D as multiplication by p^t for some t. □

COROLLARY 5.22. *Assume Hypothesis* (PO). *Then* $\mathrm{Ker}(\delta_v)$, $\mathrm{Coker}(\delta_v)$ *are both finite, of cardinalities given by*

$$\begin{aligned} \sharp\mathrm{Ker}(\delta_v) &= \sharp\mathfrak{F}(E(F_v))(p) \times \sharp H^1(\Theta, D) \\ \sharp\mathrm{Coker}(\delta_v) &= \sharp H^2(\Theta, D). \end{aligned} \tag{103}$$

PROOF. Recall, from the exact sequence (19) together with Lemma 5.3, that the kernel and cokernel of δ_v can be identified with $H^i(\Delta_\omega, E(F_{\infty,\omega}))(p)$ for $i = 1, 2$ respectively. Thus the Corollary is immediate from Lemmas 5.18, 5.19 and 5.21. □

COROLLARY 5.23. *If* $p \geq 5$ *then* $H^i(G_\infty, J_v(F_\infty)) = 0$ *for all* $i \geq 1$, *whatever type of reduction* E *has at* v.

PROOF. For the case $ord_v(j_E) \geq 0$ this is immediate from Lemmas 5.16 and 5.21, recalling that $D = 0$ if E has potential supersingular reduction at v. For the case $ord_v(j_E) < 0$ it follows from Lemma 5.16 together with the fact that $cd_p(\Delta_\omega) = 2$. This latter fact follows from 5.1, 2.2 and the assumption that $p \geq 5$. □

All that remains is to find a way to remove the terms $H^i(\Theta, D)$.

PROPOSITION 5.24. *Again assuming Hypothesis* (PO), *we have*

$$\chi(\Theta, D) = 1 \tag{104}$$

PROOF. From Lemma 5.21 we know this Euler characteristic is defined, given by

$$\chi(\Theta, D) = \prod_{0 \leq i \leq 3} \sharp H^i(\Theta, D)^{(-1)^i} \tag{105}$$

Let M_∞ denote the maximal unramified extension of $K(\mu_{p^\infty})$ contained in K_∞. Put

$$\begin{gathered} \Gamma_1 = \mathrm{Gal}(F_v(\mu_{p^\infty})/F_v), \quad \Gamma_2 = \mathrm{Gal}(M_\infty/K(\mu_{p^\infty})), \quad \Gamma_3 = \mathrm{Gal}(K_\infty/M_\infty), \\ H_1 = \mathrm{Gal}(K_\infty/F_v(\mu_{p^\infty})), \quad H_2 = \mathrm{Gal}(K_\infty/K(\mu_{p^\infty})). \end{gathered} \tag{106}$$

We will show

LEMMA 5.25. *With the hypothesis of Proposition* 5.24, *the groups* $H^i(H_1, D)$ *are finite for all* i.

Before proving this, let us note how Proposition 5.24 follows from it. Indeed, on applying the Hochschild-Serre spectral sequence

$$H^i(\Gamma_1, H^j(H_1, D)) \Rightarrow H^{i+j}(\Theta, D) \tag{107}$$

and noting that Γ_1 is topologically cyclic, of p-cohomological dimension equal to 1, we obtain exact sequences

$$0 \to H^i(H_1, D)_{\Gamma_1} \to H^{i+1}(\Theta, D) \to H^{i+1}(H_1, D)^{\Gamma_1} \to 0 \tag{108}$$

for all $i \geq 0$, and $H^0(\Theta, D) = H^0(H_1, D)^{\Gamma_1}$. Since, from the lemma, the $H^i(H_1, D)$ are finite

$$\sharp H^i(H_1, D)_{\Gamma_1} = \sharp H^i(H_1, D)^{\Gamma_1}. \tag{109}$$

Thus the left hand term of sequence (108) at the i^{th} level cancels with the right hand term of the same sequence at the $(i-1)^{\text{th}}$ level in the alternating product, (105), giving the formula for $\chi(\Theta, D)$. It just remains to prove Lemma 5.25.

PROOF OF LEMMA 5.25. First, note that since K is a finite extension of $\boldsymbol{Q}_p$ the residue field of $K(\mu_{p^\infty})$ is finite and so it is clear that $H^0(H_1, D)$ is finite. Secondly, it is sufficient to prove that the $H^i(H_2, D)$ are finite, since the index of H_2 in H_1 is prime to p and so the $H^i(H_1/H_2, D^{H_2})$ are zero for $i \geq 1$. Now E has good ordinary reduction over K and so, as in (51), there is a faithful representation ρ of H_2 which has the form

$$\rho : H_2 \hookrightarrow GL_2(\boldsymbol{Z}_p); \quad \sigma \mapsto \begin{pmatrix} \phi(\sigma)^{-1} & a(\sigma) \\ 0 & \phi(\sigma) \end{pmatrix} \tag{110}$$

(Recall that $\det(\rho)$ gives the cyclotomic character, which is trivial on H_2.) Also, as described above, the assumption that E has no complex multiplication means that a gives an isomorphism of Γ_3 with an open subgroup of $\boldsymbol{Z}_p$. Γ_2 is the direct product of $\boldsymbol{Z}_p$ with a cyclic group of order prime to p. This is because ϕ is a character mapping Γ_2 into $\boldsymbol{Z}_p^\times$. The image contains $\boldsymbol{Z}_p$ because M_∞ contains the unique unramified $\boldsymbol{Z}_p$-extension of F_v. Thus Γ_2 and Γ_3 have p-cohomological dimension equal to 1 and so the Hochschild-Serre spectral sequence gives

$$0 \to H^1(\Gamma_2, D) \to H^1(H_4, D) \to H^1(\Gamma_3, D)^{\Gamma_2} \to 0, \tag{111}$$

$$0 \to H^i(H_2, D) \to H^{i-1}(\Gamma_2, H^1(\Gamma_3, D)) \to 0, \quad \text{for all } i \geq 2. \tag{112}$$

Also, $H^1(\Gamma_2, D) = 0$. This is because Γ_2 is topologically cyclic, and thus

$$H^1(\Gamma_2, D) \cong D_{\Gamma_2}. \tag{113}$$

Since Γ_2 acts non-trivially on D, via the character ϕ, and since D is isomorphic to $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ as an Abelian group, the right hand side of (113) is zero.

Now Γ_3 acts trivially on D and thus

$$H^1(\Gamma_3, D) \cong \mathrm{Hom}(\Gamma_3, D) \tag{114}$$

which is just isomorphic to $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ as an Abelian group. Thus, by the same reasoning as we just used to show the vanishing of $H^1(\Gamma_2, D)$, the lemma will follow if we can show Γ_2 acts non-trivially on $H^1(\Gamma_3, D)$. Suppose $\tau \in \Gamma_2$, $\sigma \in \Gamma_3$. The action of Γ_2 on Γ_3 is via conjugation, $\tau \cdot \sigma = \tilde{\tau}\sigma\tilde{\tau}^{-1}$. Here, $\tilde{\tau}$ denotes a lift of τ to H_2. It is clear from the matrix calculation

$$\rho(\tilde{\tau})\rho(\sigma)\rho(\tilde{\tau})^{-1} = \begin{pmatrix} 1 & a(\sigma)/\phi(\tilde{\tau})^2 \\ 0 & 1 \end{pmatrix} \tag{115}$$

that Γ_3 is isomorphic to $\boldsymbol{Z}_p(1/\phi^2)$ as a Γ_2-module. Since $D \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p(\phi)$ as a Γ_2-module, it follows from this and (114) that

$$H^1(\Gamma_3, D) \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p(\phi^3) \tag{116}$$

as a Γ_2-module. Since ϕ gives the action of Γ_2 on D, ϕ^3 is not the trivial character. Thus $H^1(\Gamma_3, D)^{\Gamma_2}$ is finite and $H^i(\Gamma_2, H^1(\Gamma_3, D)) = 0$ for $i \geq 1$. This, together with the exact sequences (111) and (112), gives the lemma. □

Assume $p \geq 5$. If E actually has good ordinary reduction at a prime $v|p$ (not just potential good ordinary) then we may take $K = F_v$ in the above arguments. Denote the reduction of E modulo v by $\tilde{E}_v$. Then in this case, D can be identified with $\tilde{E}_{v,p^\infty}$ and

$$\mathfrak{F}(E(F_v))(p) = H^0(\Theta, D) = \tilde{E}_v(k_{F_v})(p) \tag{117}$$

COROLLARY 5.26. *Assume E has good ordinary reduction at the place v dividing p. Then Proposition* 5.24 *says*

$$\chi(\Lambda_\omega, \tilde{E}_{v,p^\infty}) \text{ is defined, equal to } 1 \tag{118}$$

where $\tilde{E}_{v,p^\infty}$ denotes the module of p-power torsion points on the reduction of E modulo v. Moreover, corollary 5.22 *now states that* $\mathrm{Ker}(\delta_v)$, $\mathrm{Coker}(\delta_v)$ *are finite with orders given by*

$$\begin{aligned} \sharp\mathrm{Ker}(\delta_v) &= \sharp\tilde{E}_v(k_{F_v})(p) \times \sharp H^1(\Lambda_\omega, \tilde{E}_{v,p^\infty}), \\ \sharp\mathrm{Coker}(\delta_v) &= \sharp H^2(\Lambda_\omega, \tilde{E}_{v,p^\infty}). \end{aligned} \tag{119}$$

Finally, from Lemma 5.21 *we have $H^3(\Lambda_\omega, \tilde{E}_{v,p^\infty}) = 0$.*

In fact, since there is no element of order 3 in the subgroup of $GL_2(\boldsymbol{Z}_3)$ formed by the upper triangular matrices, the cohomological dimension of Λ_ω equals 3 in the good ordinary case even if $p = 3$. Thus Corollary 5.26 holds for $p \geq 3$.

We conclude our discussion of the integral j-invariant case with the observation

LEMMA 5.27. *If $F = \boldsymbol{Q}$ and E actually has good ordinary reduction at p, then δ_v is a surjection.*

We omit the proof of Lemma 5.27 (see the proof of lemma 3.16 in [**4**]). It is not true in general that δ_v is a surjection, but it is true, for example, if v is unramified in F.

We complete the discussion of the local behaviour at primes dividing p with the following two lemmas which we will require later.

LEMMA 5.28. *Let K be a finite extension of $\boldsymbol{Q}_p$ and E an elliptic curve defined over K such that E has potential multiplicative reduction over K. As usual we have $K_\infty = K(E_{p^\infty})$. Let $\Omega = \mathrm{Gal}(K_\infty/K(\mu_{p^\infty}))$.*

i) *If E has split multiplicative reduction over $K(\mu_p)$ then*

$$H^1(\Omega, E(K_\infty))(p) = \boldsymbol{Q}_p/\boldsymbol{Z}_p. \tag{120}$$

ii) *Assume $p > 2$. If E has potential, but not split, multiplicative reduction over $K(\mu_p)$ then*

$$H^1(\Omega, E(K_\infty))(p) = 0. \tag{121}$$

PROOF. i) Assume E has split multiplicative reduction over K. We do not require p odd in this case. Then the module D appearing in the canonical exact sequence of G_K-modules, (82), is just $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ with the trivial action of G_K. Now both the fields K_∞ and $K(\mu_{p^\infty})$ are deeply ramified extensions of $\boldsymbol{Q}_p$. Thus, as in Proposition 5.15 above, it follows from Proposition 4.8 of [**5**] that

$$H^1(\Omega, E(K_\infty))(p) = \mathrm{Hom}(\Omega, D) \tag{122}$$

where $D = \boldsymbol{Q}_p/\boldsymbol{Z}_p$. But, as in the proof of Lemma 5.13 concerning primes not dividing p, K_∞ is obtained by adjoining to $K(\mu_{p^\infty})$ all the p^{th}-power roots of the Tate period, q_E, of E and so $\mathrm{Gal}(K_\infty/K(\mu_{p^\infty})) \cong \boldsymbol{Z}_p$. Hence (120) is clear.

ii) Assume E achieves split multiplicative reduction only over a quadratic extension K' of $K(\mu_p)$. Then (122) above is still valid, but now $G_{K(\mu_p)}$ acts on D via the non-trivial character of $\mathrm{Gal}(K'/K(\mu_p))$. Then this case is deduced from the first case exactly as in the proof of Lemma 5.13, earlier. □

LEMMA 5.29. *If $p \geq 3$ then take $K = F_0$, if $p = 2$ take $K = F_1$. Suppose v is a prime of F at which $\mathrm{ord}_v(j_E) < 0$. Then E attains split multiplicative reduction over $K_{v'}$, where v' is a prime of K dividing v.*

PROOF. As explained in Lemma V.5.2 of [**46**], since E has potential split multiplicative reduction there is a Tate curve, E_q/F, which is a quadratic twist of E and thus the action of the absolute Galois group of $K_{v'}$ on points of E is given by the action on points of E_q twisted by a quadratic character, τ. Then the action of the absolute Galois group of $K_{v'}$ on the Galois module D appearing in the exact sequence (82) is entirely via the quadratic character, τ. This is because D is the Kummer group generated by the p^{th}-power roots of the Tate period, q. But the Galois action on D also filters through $\mathrm{Gal}(K_{v'}(E_{p^\infty})/K_{v'})$, the decomposition group at v' of $\mathrm{Gal}(F(E_{p^\infty})/K)$. By the assumption that $K = F_0$ if $p \geq 3$ (resp. F_1 if $p = 2$) this latter Galois group is contained in the subgroup of matrices congruent to 1 modulo p (resp. 1 modulo 4) so contains no 2-torsion. Thus the absolute Galois group of $K_{v'}$ acts on D trivially and so maps identically to 1 under the quadratic character, τ. But this means that the extension of $K_{v'}$ over which E is isomorphic to E_q is of degree 1, that is E has split multiplicative reduction over $K_{v'}$. □

6. Relationship with the cyclotomic theory.

We explain the relationship between Conjecture 2.4 and the corresponding conjecture in the cyclotomic theory. This gives some criteria under which we can prove Conjecture 2.4. We freely admit that these results are rather weak. However, as was pointed out to us by R. Greenberg, we can at last finally give some concrete examples where Conjectures 1.3 and 1.4 can be proven. Recall, if L is a finite extension of $\boldsymbol{Q}$, we write L^{cyc} for the cyclotomic $\boldsymbol{Z}_p$-extension of L.

First recall that the analogue of Conjecture 2.4 for the cyclotomic $\boldsymbol{Z}_p$-extension is long standing, originally due to Mazur in the ordinary case [**29**].

CONJECTURE 6.1. *If* $\Gamma = \mathrm{Gal}(F^{cyc}/F)$ *then, for every prime* p,

$$\Lambda(\Gamma)\text{-rank}(\mathscr{C}_p(E/F^{cyc})) = \tau_p(E/F) \tag{123}$$

Here, at the F_∞ level, $\mathscr{C}_p(E/F^{cyc})$ denotes the Pontrjagin dual of $\mathscr{S}_p(E/F^{cyc})$. Recall Proposition 3.4 relating 2.4 to the surjectivity of certain localisation maps. Analogously, we have

PROPOSITION 6.2. *In the sequence defining* $\mathscr{S}_p(E/F^{cyc})$

$$0 \longrightarrow \mathscr{S}_p(E/F^{cyc}) \longrightarrow H^1(F^S/F^{cyc}, E_{p^\infty}) \xrightarrow{\lambda_{F^{cyc}}} \bigoplus_{v \in S} J_v(F^{cyc}) \tag{124}$$

if the above Conjecture 6.1 *is true, then the map* $\lambda_{F^{cyc}}$ *is a surjection.*

Here $J_v(F^{cyc})$ is defined analogously to the definition of $J_v(F_\infty)$ in (15). The proof of Proposition 6.2 is well known and is entirely analogous to the proof of 3.4. It is worth pointing out though that in this case 6.2 is not an if and only if statement. The problem is that we do not now have the full strength of Theorem 3.5, only a lower bound. To get equality one would have to prove the so called 'Weak Leapoldt Conjecture', which asserts that $H^2(F^S/F^{cyc}, E_{p^\infty}) = 0$ for p odd. We assume for the rest of this section that $p \geq 5$.

COROLLARY 6.3. *Suppose Conjecture* 6.1 *holds for* F *replaced by every finite extension of* F *contained in* F_∞, *and assume* p *is at least* 5. *Then Conjecture* 2.4 *holds.*

PROOF. From Proposition 6.2, the hypothesis of the corollary implies $\lambda_{K^{cyc}}$ is a surjection for any finite extension K, contained in F_∞. But

$$H^1(F^S/F_\infty, E_{p^\infty}) = \varinjlim H^1(F^S/K^{cyc}) \tag{125}$$

$$J_v(F_\infty) = \varinjlim J_v(K^{cyc}) \tag{126}$$

where the inductive limits are taken over all such K with respect to the

canonical restriction maps. Hence so λ_{F_∞} is an inductive limit of the surjections $\lambda_{K^{cyc}}$, and thus is itself a surjection. The corollary then follows from Proposition 3.4. □

Corollary 6.3 does not give a very practically applicable method for proving Conjecture 1.3 in general. The situation is improved if we strengthen the condition on $\mathscr{C}_p(E/F^{cyc})$, assuming not only that it is $\Lambda(\Gamma)$-torsion, but also that it has μ-invariant equal to 0. We recall what this means. Let Γ denote any profinite group which is isomorphic to $\boldsymbol{Z}_p$, and let $\Lambda(\Gamma)$ denote the Iwasawa algebra of Γ. We recall that $\Lambda(\Gamma)$ is topologically isomorphic to the ring of formal power series $\boldsymbol{Z}_p[[T]]$ in an indeterminate T with coefficients in $\boldsymbol{Z}_p$. If X is a finitely generated $\Lambda(\Gamma)$-module which is $\Lambda(\Gamma)$-torsion, then we say X has μ-invariant zero if its characteristic power series is not divisible by p in $\boldsymbol{Z}_p[[T]]$. It is easy to see that the following two assertions are equivalent for any finitely generated $\Lambda(\Gamma)$-module, X:

i) X is a finitely generated $\boldsymbol{Z}_p$-module

ii) X is $\Lambda(\Gamma)$-torsion and has μ-invariant zero.

Define, for $n \geq 0$,

$$H = \mathrm{Gal}(F_\infty/F^{cyc}), \quad H_n = \mathrm{Gal}(F_\infty/F_n^{cyc}) \quad \text{and} \quad \Gamma_n = \mathrm{Gal}(F_n^{cyc}/F_n). \tag{127}$$

The field F_n^{cyc} is simply $F(E_{p^{n+1}}, \mu_{p^\infty})$, as F_0 contains the p^{th} roots of unity. Then H_0 is pro-p and contains no element of order p. Defining $\Lambda(H_0)$ in the usual manner, Theorem 2.3 is true with $\Lambda(R)$ replaced by $\Lambda(H_0)$ and so we can define the $\Lambda(H_0)$-rank of a finitely generated $\Lambda(H)$-module exactly analogously to the definition of $\Lambda(R)$-rank in (10). Then H acts continuously on $\mathscr{S}_p(E/F_\infty)$ making it into a discrete $\Lambda(H)$-module.

THEOREM 6.4. *Assume that* $p \geq 5$.

i) *If* $\mathscr{C}_p(E/F_\infty)$ *is a finitely generated* $\Lambda(H)$*-module, then* $\mathscr{C}_p(E/L^{cyc})$ *is a finitely generated* $\boldsymbol{Z}_p$*-module for each finite extension* L *of* F *which is contained in* F_∞.

ii) *Conversely, assume that there exists a finite extension* L *of* F *which is contained in* F_∞ *such that* $\mathrm{Gal}(F_\infty/L)$ *is a pro-p group and* $\mathscr{C}_p(E/L^{cyc})$ *is a finitely generated* $\boldsymbol{Z}_p$*-module. Then* $\mathscr{C}_p(E/F_\infty)$ *is a finitely generated* $\Lambda(H)$*-module, which is* $\Lambda(R)$*-torsion, where we recall* $R = \mathrm{Gal}(F_\infty/F_0)$.

This shows that the natural analogue to $\Lambda(R)$-modules of finitely generated $\Lambda(\Gamma)$-modules being torsion and having μ-invariant zero is that they should be finitely generated over $\Lambda(H)$. In the next section, we will give examples where $\mathscr{C}_p(E/F_\infty)$ is finitely generated over $\Lambda(H)$, and where it is not.

Before giving the proof of Theorem 6.4 we note some obvious, but interesting, corollaries.

COROLLARY 6.5. *Assume $p \geq 5$. If $\mathcal{C}_p(E/L^{cyc})$ is a finitely generated $\boldsymbol{Z}_p$-module for some finite extension L of F contained in F_∞ with $\mathrm{Gal}(F_\infty/L)$ a pro-p group, then the same is true for all finite extensions of F contained in F_∞.*

COROLLARY 6.6. *If $p \geq 5$ is any prime such that $\mathcal{C}_p(E/F^{cyc})$ is not a finitely generated $\boldsymbol{Z}_p$-module, then $\mathcal{C}_p(E/F_\infty)$ is not a finitely generated $\Lambda(H)$-module.*

We now give the proof of Theorem 6.4.

PROOF. We start with part i) and assume that $\mathcal{C}_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module. Thus, for some integer $m \geq 1$, there is a surjection

$$\Lambda(H)^m \twoheadrightarrow \mathcal{C}_p(E/F_\infty). \tag{128}$$

Let Ω be the subgroup of H fixing L^{cyc}. Since L is of finite degree over F, Ω is of finite index, d say, in H. Taking Ω coinvariants of (128) and using the fact that $(\Lambda(H)^m)_\Omega$ is a free $\boldsymbol{Z}_p$-module, of rank md, there is a surjection

$$\boldsymbol{Z}_p^{md} \twoheadrightarrow \mathcal{C}_p(E/F_\infty)_\Omega, \tag{129}$$

and so $\mathcal{S}_p(E/F_\infty)^\Omega$ has finite $\boldsymbol{Z}_p$-corank.

Consider the following diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{S}_p(E/F_\infty)^\Omega & \longrightarrow & H^1(F^S/F_\infty, E_{p^\infty})^\Omega & \xrightarrow{\phi_\infty} & \left(\bigoplus_{v\in S} J_v(F_\infty)\right)^\Omega \\ & & \uparrow f & & \uparrow g & & \uparrow h \\ 0 & \longrightarrow & \mathcal{S}_p(E/L^{cyc}) & \longrightarrow & H^1(F^S/L^{cyc}, E_{p^\infty}) & \longrightarrow & \bigoplus_{v\in S} J_v(L^{cyc}) \end{array} \tag{130}$$

In Lemma 6.7 following, we will show $\mathrm{Ker}(f)$ is finite and $\mathrm{Coker}(f)$ has finite $\boldsymbol{Z}_p$-corank. Given this it follows from (129) that $\mathcal{C}_p(E/L^{cyc})$ has finite $\boldsymbol{Z}_p$-rank, proving i).

We next assume the hypotheses of ii) are valid. The fact that $\mathcal{C}_p(E/L^{cyc})$ is a finitely generated $\boldsymbol{Z}_p$-module together with lemma 6.7 below (that $\mathrm{Ker}(f)$ and $\mathrm{Coker}(f)$ have finite $\boldsymbol{Z}_p$-corank) gives that $\mathcal{S}_p(E/F_\infty)^\Omega$ has finite $\boldsymbol{Z}_p$-corank. Moreover, as $\mathrm{Gal}(F_\infty/L)$ is pro-p it follows that the subgroup Ω is also pro-p. Since $\mathcal{C}_p(E/F_\infty)$ is compact we may apply the Nakayama Lemma 2.6 to conclude that$\mathcal{C}_p(E/F_\infty)$ is a finitely generated $\Lambda(\Omega)$-module. But Ω is a subgroup of H and thus $\mathcal{C}_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module. It only remains to remark that any finitely generated $\Lambda(R)$-module which is finitely generated as a $\Lambda(H)$-module must be $\Lambda(R)$-torsion. This follows because H_0 has infinite index in R and so $\Lambda(R)$ is not a finitely generated $\Lambda(H_0)$-module, but H_0 has finite index in H and so any finitely generated $\Lambda(H)$-module is also finitely generated as a $\Lambda(H_0)$-module. (Note that H itself is in general not a subgroup of R.) □

LEMMA 6.7. *The following assertions hold for the diagram* (130):

i) *The kernel and cokernel of g are both finite.*

ii) *Assume* $p \geq 5$. *Then the kernel of h has finite* $\boldsymbol{Z}_p$*-corank, at most equal to r where r is the (finite) number of primes of* $L(\mu_{p^\infty})$ *at which E has split multiplicative reduction. Also,* $\mathrm{Coker}(h)$ *is finite.*

iii) *Assume* $p \geq 5$. *If L contains* $F(\mu_p)$ *then the kernel of h has* $\boldsymbol{Z}_p$*-corank exactly equal to the number r defined in part* ii).

iv) *Assume* $p \geq 5$. *Then* $\mathrm{Ker}(f)$ *is finite and* $\mathrm{Coker}(f)$ *has finite* $\boldsymbol{Z}_p$*-corank, at most equal to the number r defined in part* ii).

PROOF. i) By the inflation restriction exact sequence

$$\mathrm{Ker}(g) = H^1(\Omega, E_{p^\infty}) \quad \text{and} \quad \mathrm{Coker}(g) \subset H^2(\Omega, E_{p^\infty}). \tag{131}$$

These are both shown to be finite in the appendix to [**10**], see also [**9**]. The essential idea is that the Lie algebra of Ω is the semisimple Lie algebra $sl_2(\boldsymbol{Q}_p)$ for which V_pE is a simple, finite dimensional and non-trivial representation. Thus

$$H^i(\mathrm{Lie}(\Omega), V_pE) = 0, \quad \text{for all } i \geq 0, \tag{132}$$

from which part i) follows, by a theorem of Lazard (see Theorem V.2.4.10 in [**28**]) relating it to (132).

ii) We first remark that since there are only finitely many primes of L^{cyc} above any prime of L, and since E has non-integral j-invariant at only finitely many primes of L, the number r is finite. As in the local analysis above, used to prove Theorem 1.1, and in particular as in Lemma 2.8

$$\mathrm{Ker}(h) = \bigoplus_{v|S} H^1(\Omega_\omega, E(F_{\infty,\omega}))(p) \tag{133}$$

where v now runs over the primes of L^{cyc} dividing S and for each such v, ω is a prime of F_∞ dividing v, and Ω_ω the decomposition group of Ω at ω. Similarly,

$$\mathrm{Coker}(h) = \bigoplus_{v|S} H^2(\Omega_\omega, E(F_{\infty,\omega}))(p) \tag{134}$$

Suppose first that v does not divide p. Then, as in the proof of Lemma 5.13 above, we need to analyse the $H^i(\Omega_\omega, E_{p^\infty})$ for $i \geq 1$. If v is a potentially multiplicative prime then we showed in Lemma 5.13 that $H^1(\mathrm{Gal}(F_{\infty,\omega}/L(\mu_{p^\infty})_\omega), E_{p^\infty})$ is either 0 or isomorphic to $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. Then a simple argument with the inflation-restriction exact sequence shows that $H^1(\Omega_\omega, E_{p^\infty})$ has $\boldsymbol{Z}_p$-corank at most equal to 1. Since Ω_ω is isomorphic to the semidirect product of a group isomorphic to $\boldsymbol{Z}_p$ with a finite cyclic group of order prime to p it follows by cohomological dimension that $H^2(\Omega_\omega, E_{p^\infty}) = 0$ in this case. If E has potential good reduction at v then, since both L_v^{cyc} and $F_{\infty,\omega}$ contain the unramified

$\mathbf{Z}_p$-extension of L_v, it follows from the work of Serre-Tate [**45**] that Ω_ω is finite and of order prime to p. Thus $H^i(\Omega_\omega, E_{p^\infty}) = 0$ in this case, for $i = 1$ or 2.

Next assume that v does divide p. Then as in the proof of Lemma 5.28 above, since both L_v^{cyc} and $F_{\infty,\omega}$ are deeply ramified extensions of L_v, we have

$$H^i(\Omega_\omega, E(F_{\infty,\omega}))(p) = H^i(\Omega_\omega, D), \quad i \geq 1 \tag{135}$$

where D is the Galois module defined in (82). If E has potential supersingular reduction at v then $D = 0$ and we are done. If E has potential ordinary reduction at v then we showed in Lemma 5.25 that $H^i(K_\infty/L_v^{cyc}, D)$ is finite for all $i \geq 1$, where K denotes a finite extension of L_v over which E acquires good reduction and such that $|K : L_v|$ is prime to p. It follows from the Hochschild-Serre spectral sequence that $H^i(\Omega_\omega, D)$ is finite for all $i \geq 1$. Finally, if E has potential multiplicative reduction at v then that $H^1(\Omega_\omega, D)$ has $\mathbf{Z}_p$-corank at most 1 follows from Lemma 5.28 as in the case of primes $v \nmid p$ above. Similarly the argument that $H^2(\Omega_\omega, D) = 0$ is identical to that above.

iii) This exact value of the $\mathbf{Z}_p$-corank follows by the same arguments as those above for part ii) where the only point at which we failed to give the exact value of the $\mathbf{Z}_p$-corank was in using the inflation-restriction exact sequence to obtain an upper bound on the $\mathbf{Z}_p$-coranks of the cohomology groups for the extension $F_{\omega,\infty}/L_v^{cyc}$ from the corresponding cohomology groups for the extension $F_{\omega,\infty}/L(\mu_{p^\infty})_\omega$ whose $\mathbf{Z}_p$-coranks we know explicitly from Lemmas 5.13 and 5.28. If L contains $F(\mu_p)$ then these extensions are the same. The only other observation necessary is to note that E has split multiplicative reduction at a prime ω of $L(\mu_{p^\infty})$ if and only if E has split multiplicative reduction over $L(\mu_p)_\omega$, because $p > 2$.

Finally, assertion iv) now follows immediately from diagram (130), by the snake lemma. □

The following lemma follows from the above analysis of diagram (130).

LEMMA 6.8. *Assume $p \geq 5$. If $\mathcal{C}_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module then*

$$\mathbf{Z}_p\text{-rank}(\mathcal{C}_p(E/F_n^{cyc})) = O(p^{3n}) \quad \text{as } n \to \infty. \tag{136}$$

PROOF. The upper bound

$$\mathbf{Z}_p\text{-corank}(\mathcal{S}_p(E/F_\infty)^{H_n}) = O(p^{3n}) \quad \text{as } n \to \infty, \tag{137}$$

follows immediately from the asymptotic theorem (Lemma 3.4.1 in [**19**].) Upon substituting $L = F_n$ into diagram (130) and using Lemma 6.7 this translates into the upper bound required in (136). The only extra observation required for this is that for a prime v of F such that $ord_v(j_E) < 0$, if r_n equals the number of

primes of F_n^{cyc} above v then $r_n = O(p^{2n})$. This is because the decomposition group Δ_ω, for any prime $\omega|v$, has dimension equal to 2 as a p-adic Lie group, by Lemma 5.1. Thus

$$\boldsymbol{Z}_p\text{-corank}(\text{Coker}(\mathscr{S}_p(E/F_n^{cyc}) \to \mathscr{S}_p(E/F_\infty)^{H_n})) = O(p^{2n}). \tag{138}$$

□

We can do much better, however. The full strength of Theorem 3.1 in [**18**] describes the $\boldsymbol{Z}_p$-rank precisely in this situation. Recall that if Y is a finitely generated, torsion $\Lambda(\Gamma)$-module then the λ-invariant of Y, which we denote by $\lambda_{inv}(Y)$, is equal to the $\boldsymbol{Z}_p$-rank of $Y/Y(p)$. Then Theorem 3.1 in [**18**] describes exactly how the λ-invariant of $\mathscr{C}_p(E/F_n^{cyc})$ changes as n increases, under certain conditions.

Let B_n denote the kernel of the reduction map from $GL_2(\boldsymbol{Z}_p)$ to the $GL_2(\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})$. Since G_∞ is an open subgroup of $GL_2(\boldsymbol{Z}_p)$ it is clear that we have

$$\text{Gal}(F_\infty/F_n) = B_n \tag{139}$$

for all sufficiently large n.

PROPOSITION 6.9. *Assume* i) $p \geq 5$, ii) G_∞ *is a pro-p group and* iii) $\mathscr{C}_p(E/F^{cyc})$ *is a finitely generated* $\boldsymbol{Z}_p$*-module. Let* $r(n)$ *denote the number of primes of* F_n^{cyc} *not dividing p and at which E has split multiplicative reduction. Let m be the smallest non-negative integer such that* (139) *is valid. Then, for* $n \geq m$,

$$\lambda_{inv}(\mathscr{C}_p(E/F_n^{cyc})) = Np^{3(n-m)} - r(n) \tag{140}$$

where

$$N = \lambda_{inv}(\mathscr{C}_p(E/F_m^{cyc})) + r(m). \tag{141}$$

PROOF. Under the hypotheses of the proposition, the formula of [**18**] applies to give

$$\lambda_{inv}(\mathscr{C}_p(E/F_n^{cyc})) = |F_n^{cyc} : F_m^{cyc}|\lambda_{inv}(\mathscr{C}_p(E/F_n^{cyc})) + \sum_{\omega \in P}(e_{n,m}(\omega) - 1) \tag{142}$$

where P consists of the set of primes, ω, of F_n^{cyc} such that $\omega \not| p$ and E has split multiplicative reduction at ω. The number $e_{n,m}(\omega)$ denotes the ramification index of ω in the extension F_n^{cyc}/F_m^{cyc}. (There is a third term in the general formula, but this gives no contribution for the extension F_n/F_m.) Since the primes ω in P do not divide p, the extension $F_{n,\omega}^{cyc}/F_{m,\omega}^{cyc}$ is totally ramified. Also, since this extension is a p extension and we assumed $p \geq 5$, E has split multiplicative reduction over $F_{n,\omega}^{cyc}$ if and only if E has split multiplicative reduction

over $F_{m,\omega}^{cyc}$. Thus P consists simply of the $r(n)$ primes of F_n^{cyc} dividing the $r(m)$ primes of F_m^{cyc} which do not divide p and at which E has split multiplicative reduction. Therefore

$$\sum_{\omega \in P}(e_{n,m}(\omega) - 1) = |F_n^{cyc} : F_m^{cyc}|r(m) - r(n), \tag{143}$$

and formula (140) follows from the choice of m satisfying (139). Indeed, for n at least m, it follows from (139) that F_{n+1} has degree exactly p^4 over F_n. But, as it is also clear from (139) that the Galois group of F_{n+1} over F_n has exponent p, it follows easily from the Weil pairing that the intersection of F_n^{cyc} with F_{n+1} must be precisely the field generated over F^n by the $p^{n+2^{\text{th}}}$ roots of unity. But then we conclude that $|F_{n+1}^{cyc} : F_n^{cyc}| = p^3$ for all n at least m. This completes the proof of Proposition 6.9. □

COROLLARY 6.10. *Assume the hypotheses of Proposition* 6.9 *and let* $r(n)$ *and* m *be as defined there. Assume also that* E *has potential good reduction at all primes* v *of* F *dividing* p. *Then for all* $n \geq m$

$$\boldsymbol{Z}_p - \text{rank}(\mathscr{C}_p(E/F_\infty)_{H_n}) = Np^{3(n-m)} \tag{144}$$

where N *is as defined in* (141) *above. Thus* $\mathscr{C}_p(E/F_\infty)$ *is a finitely generated* $\Lambda(H_0)$*-module of* $\Lambda(H_0)$*-rank equal to*

$$\frac{N}{|H_0 : H_m|} \tag{145}$$

PROOF. In the fundamental diagram (130) relating the F_∞ level with the cyclotomic level we take $L = F_n$ and $\Omega = H_n$. The assumption that $\mathscr{C}_p(E/F^{cyc})$ is a finitely generated $\boldsymbol{Z}_p$-module, together with the assumption that G_∞ is a pro-p group, implies, by Corollary 6.5, that $\mathscr{C}_p(E/F_n^{cyc})$ is $\Lambda(\Gamma_n)$-torsion. It follows from Proposition 6.2 that the bottom right hand horizontal map in (130) is a surjection. The assumption that G_∞ is pro-p implies that F contains μ_p. Then, from parts i) and iii) of Lemma 6.7 and the assumption that E has potential good reduction at all $v|p$, the term $-r(n)$ appearing in (140) is perfectly corrected by the diagram (130), giving the first part of the corollary. The final statement of the corollary then follows from the asymptotic formula, Lemma 3.4.1, in [**19**]. □

We end this section with a number of general remarks. Firstly, we want to make clear our indebtedness to the very interesting paper [**18**] of Hachimori and Matsuno for suggesting to us the results of this section. Secondly, we believe that our results indicate parallels between the present GL_2 Iwasawa Theory and certain classical phenomena in the Iwasawa Theory of $\boldsymbol{Z}_p$-extensions. Let us

assume that p is odd, and recall that

$$F_0 = F(E_p), \quad R = \mathrm{Gal}(F_\infty/F_0), \quad \text{and} \quad H_0 = \mathrm{Gal}(F_\infty/F_0(\mu_{p^\infty})). \tag{146}$$

As we have already remarked, both $\Lambda(R)$ and $\Lambda(H_0)$ are Noetherian and have no divisors of zero, and so possess skew fields of fractions. We can therefore define the rank of a module over these Iwasawa algebras in the usual fashion (see (10).) Let X be a finitely generated, torsion $\Lambda(R)$-module. We believe, in view of Theorem 6.4, that the GL_2 property parallel to being torsion and having μ-invariant zero in the theory of $\boldsymbol{Z}_p$-extensions should be that X is finitely generated over $\Lambda(H_0)$. Similarly, it seems reasonable to expect that the $\Lambda(H_0)$-rank of X should be analogous to the λ-invariant in the theory of $\boldsymbol{Z}_p$-extensions. In §7 we will exhibit an example of an elliptic curve where $\mathscr{C}_p(E/F_\infty)$ fails to be finitely generated over $\Lambda(H_0)$ and yet still has finite $\Lambda(H_0)$-rank.

QUESTION. Assume E has potential good ordinary reduction at all primes of F dividing p. If we take $X = \mathscr{C}_p(E/F_\infty)$ then does X always have finite $\Lambda(H_0)$-rank?

It would also be interesting to exhibit elliptic curves E over F and primes p with $\mathscr{C}_p(E/F)$ finite such that $\mathscr{C}_p(E/F_\infty)$ has $\Lambda(H_0)$-rank equal to zero. Corollary 6.10 gives some specific conditions which would guarantee this. They are not necessary, however, as this corollary only concerns the case where $\mathscr{C}_p(E/F_\infty)$ is finitely generated as a $\Lambda(H_0)$-module.

7. Examples.

We can finally give the first concrete examples where Conjecture 1.3 can be proven and thus all the hypotheses of Theorem 1.1 are satisfied, namely the $\boldsymbol{Q}$ isogeny class of elliptic curves of conductor 11 at the prime p equals 5. In order to prove Conjecture 1.3 for all three isogenous curves, we prove the isogeny invariance of the more general Conjecture 2.4.

EXAMPLE. Consider the curve, 11(A3) in Cremona's tables [**11**], of conductor 11. It has minimal Weierstraß equation

$$E : y^2 + y = x^3 - x^2 \tag{147}$$

and is the elliptic curve corresponding to the modular group $\Gamma_1(11)$. It is more usually denoted $X_1(11)$. It does not admit complex multiplication and thus is relevant to the discussion in this paper. Serre has shown, in [**41**], that $G_\infty = GL_2(\boldsymbol{Z}_p)$ for all $p \neq 5$, and so Theorem 6.4 is difficult to apply in these cases. For $p = 5$, however, the situation is more hopeful as $X_1(11)$ has a rational point of order 5. It follows that E_5 fits into the exact sequence

$$0 \to \boldsymbol{Z}/5\boldsymbol{Z} \to E_5 \to \mu_5 \to 0. \tag{148}$$

In fact, this sequence does not split and $\boldsymbol{Q}(E_5)$ is a degree 5 extension of $\boldsymbol{Q}(\mu_5)$. Indeed (148) does not even split as an exact sequence of $\mathrm{Gal}(\overline{\boldsymbol{Q}_{11}}/\boldsymbol{Q}_{11})$-modules, because E has split multiplicative reduction at 11 with the 11-adic Tate period, q_E, having order 1 at 11. We shall apply the second part of Theorem 6.4 with $L = \boldsymbol{Q}(\mu_5)$, since $\mathrm{Gal}(F_\infty/L)$ is a pro-5 group. Clearly, though, the crux is to show it satisfies the condition that $\mathscr{C}_p(E/\boldsymbol{Q}(\mu_{p^\infty}))$ is a finitely generated $\boldsymbol{Z}_5$-module. The hypothesis that $\mathscr{C}_p(E/\boldsymbol{Q}(\mu_{5^\infty}))$ be $\Lambda(\Gamma)$-torsion presents no problem as our ground field is $\boldsymbol{Q}(\mu_5)$, an Abelian extension of $\boldsymbol{Q}$, and so we could appeal to recent work of Kato's referred to earlier. The condition that it has μ-invariant equal to zero requires a more subtle analysis. A classical descent argument, carried out in [**10**], gives

THEOREM 7.1.

$$\mathscr{S}_5(E/\boldsymbol{Q}(\mu_5)) = 0, \quad E(\boldsymbol{Q}(\mu_5))(5) = \boldsymbol{Z}/5\boldsymbol{Z}. \tag{149}$$

Then for $E = X_1(11)$, $p = 5$, $F = \boldsymbol{Q}(\mu_5)$ we have

$$\begin{aligned} \sharp(\tilde{E}(k_F)(5)) = 5, \quad Ш(E/F)(5) = 0, \\ \sharp E(F)(5) = 5, \quad c_{11}(E) = 1, \end{aligned} \tag{150}$$

and E has good reduction at all primes not dividing 11. Thus $\rho_5(E/F) = 1$ in this case. It follows from 5.7 that $\chi(\Gamma, \mathscr{S}_5(E/\boldsymbol{Q}(\mu_{5^\infty})))$ is defined and equal to 1. Here $\Gamma = \mathrm{Gal}(\boldsymbol{Q}(\mu_{5^\infty})/F)$. But since this gives the leading term for a characteristic power series for $\mathscr{S}_5(E/\boldsymbol{Q}(\mu_{5^\infty}))$, it follows that the characteristic power series must be a unit in $\Lambda(\Gamma)$.

COROLLARY 7.2. *The 5^∞-Selmer group $\mathscr{S}_5(X_1(11)/\boldsymbol{Q}(\mu_{5^\infty}))$ is finite and so, in particular, has μ-invariant equal to zero.*

(In fact, one can show that $\mathscr{S}_5(X_1(11)/\boldsymbol{Q}(\mu_{5^\infty})) = 0$, see [**10**].) It follows that we have satisfied all the conditions of Theorem 6.4 and so can conclude:

COROLLARY 7.3. *For $E = X_1(11)$, $\mathscr{C}_5(X_1(11)/\boldsymbol{Q}(E_{5^\infty}))$, is $\Lambda(R)$-torsion of finite $\Lambda(H_0)$-rank, where $H_0 = \mathrm{Gal}(F_\infty/F_0^{cyc})$, as above. It follows that $X_1(11)$ satisfies all the conditions to apply Theorem* 1.1 *at the prime $p = 5$ taking as ground field either $F = \boldsymbol{Q}$ or $F = \boldsymbol{Q}(\mu_5)$.*

A simpler 5-descent on E, described by Greenberg in [**15**], shows that

$$Ш(E/\boldsymbol{Q})(5) = 0, \quad E(\boldsymbol{Q}) = \boldsymbol{Z}/5\boldsymbol{Z}. \tag{151}$$

Also, for this E over $\boldsymbol{Q}$ the set $\mathfrak{M}$ and corresponding Euler factors appearing in

the full Euler characteristic formula in Theorem 1.1 consists of just

$$\mathfrak{M} = \{11\}, \quad L_{11}(X_1(11), s) = (1 - 11^s)^{-1}. \tag{152}$$

Thus Theorem 1.1 gives

COROLLARY 7.4. *Denote by $G_\infty(F)$ the Galois group F_∞/F. For $F = \boldsymbol{Q}$ and $p = 5$ we have*

$$\chi(G_\infty(\boldsymbol{Q}), \mathscr{S}_5(X_1(11)/\boldsymbol{Q}(E_{5^\infty}))) = 5. \tag{153}$$

Similarly, for $F = \boldsymbol{Q}(\mu_5)$, we deduce from (150) *that*

$$\chi(G_\infty(\boldsymbol{Q}(\mu_5)), \mathscr{S}_5(X_1(11)/\boldsymbol{Q}(E_{5^\infty}))) = 5^4. \tag{154}$$

The only extra observation required to prove (154) is that 11 splits completely in $\boldsymbol{Q}(\mu_5)$ and $L_v(E, s) = (1 - 11^{-s})^{-1}$ for each of the *four* primes v of $\boldsymbol{Q}(\mu_5)$ dividing 11.

We confess that we are currently unable to apply Theorem 1.1 to calculate the G_∞-Euler characteristic for $E = X_1(11)$ at a single ordinary prime $p \geq 7$.

We complete our discussion of the curve $X_1(11)$ at $p = 5$ by making some further observations about the asymptotic behaviour of $\mathscr{C}_5(X_1(11)/\boldsymbol{Q}(E_{5^{n+1}})^{cyc})$, as $n \to \infty$. We know from Corollaries 6.5 and 7.2 that $\mathscr{C}_5(X_1(11)/\boldsymbol{Q}(E_{5^{n+1}})^{cyc})$ is a finitely generated $\boldsymbol{Z}_p$-module for all $n \geq 0$.

From now until the end of Corollary 7.7 we take E to be $X_1(11)$, and recall that, with this choice of E,

$$F = \boldsymbol{Q}(\mu_5), \quad F_n = \boldsymbol{Q}(E_{5^{n+1}}), \quad F_n^{cyc} = \boldsymbol{Q}(E_{5^{n+1}}, \mu_{5^\infty}). \tag{155}$$

PROPOSITION 7.5. *We now have $\lambda_{inv}(\mathscr{C}_5(X_1(11)/F_0^{cyc})) = 16$, and*

$$\lambda_{inv}(\mathscr{C}_5(X_1(11)/F_n^{cyc})) = 4 \times 5^{3n} - 4 \times 5^{2n-1} \quad (n \geq 1). \tag{156}$$

PROOF. We begin by describing the image of $\mathrm{Gal}(F_\infty/\boldsymbol{Q})$ in the automorphism group of $T_5X_1(11)$. Now E_{5^∞} contains a unique cyclic subgroup Φ of order 5^2, which is stable under the action of $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$, and which contains the subgroup of order 5 generated by $(0, 0)$. Pick a basis e_1, e_2 of T_5E such that the projection of e_1 in E_{5^2} generates this subgroup Φ. For each σ in $\mathrm{Gal}(F_\infty/\boldsymbol{Q})$, we have

$$\sigma(e_1) = ae_1 + ce_2, \quad \sigma(e_2) = be_1 + de_2, \tag{157}$$

and this clearly defines an injection of $\mathrm{Gal}(F_\infty/\boldsymbol{Q})$ into the subgroup W of $GL_2(\boldsymbol{Z}_5)$ consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \equiv 0 \mod 5^2$, $a \equiv 1 \mod 5$. Now Lang and Trotter [**27**] have explicitly determined the image of $\mathrm{Gal}(F_\infty/\boldsymbol{Q})$

in $T_5X_0(11)$. By analysing the behaviour of the image under isogeny, one deduces easily that the image of $\mathrm{Gal}(F_\infty/\boldsymbol{Q})$ in $T_5X_1(11)$ is the whole of W. It is then clear that $G_\infty = \mathrm{Gal}(F_\infty/F)$ can be identified with the subgroup U of W consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \equiv 0 \bmod 5^2$, $a \equiv d \equiv 1 \bmod 5$. It follows easily from this explicit description that $|F_0^{cyc} : F^{cyc}| = 5$, $|F_1^{cyc} : F_0^{cyc}| = 5^2$ and $|F_{n+1}^{cyc} : F_n^{cyc}| = 5^3$ for $n \geq 1$. Hence we obtain that $|F_n^{cyc} : F| = 5^{3n}$ for all $n \geq 1$. We recall that 11 is the only prime at which $X_1(11)$ has split multiplicative reduction. As earlier, let $r(n)$ denote the number of primes of F_n^{cyc} lying above 11. We claim that

$$r(0) = 4, \quad r(n) = 4 \times 5^{2n-1} \quad (n \geq 1), \tag{158}$$

and that each of these primes has absolute ramification index equal to 5^{n+1} for all $n \geq 0$. To justify this, we note that if v denotes any prime of F_n^{cyc} above 11 then the 11-adic Tate curve shows that

$$F_{n,v}^{cyc} = \boldsymbol{Q}_{11}(\mu_{5^\infty}, q^{1/5^{n+1}}), \tag{159}$$

where q denotes the 11-adic Tate period of E. As $X_1(11)$ has discriminant -11, q has order 1 at 11, and so it is clear that $F_{n,v}^{cyc}$ has absolute ramification index 5^{n+1}. Moreover, 11 splits completely in F, and then each of the four primes of F above 11 are inert in F^{cyc}. No residue field extension of degree a power of 5 is possible above the field $\boldsymbol{Q}_{11}(\mu_{5^\infty})$, since this field is the unique unramified $\boldsymbol{Z}_5$-extension of $\boldsymbol{Q}_{11}$. These remarks prove the above formulae for $r(n)$. The assertion of Proposition 7.5 now follows immediately from the main result of Hachimori-Matsuno [**18**] applied to $X_1(11)$ for the 5-extension F_n/F, recalling that $\mathcal{S}_5(X_1(11)/F^{cyc}) = 0$.

COROLLARY 7.6. *Let $H_n = \mathrm{Gal}(F_\infty/F_n^{cyc})$. Then, for all $n \geq 0$, we have*

$$\boldsymbol{Z}_5\text{-rank}(\mathcal{C}_5(X_1(11)/F_\infty)_{H_n}) = 4 \times 5^{3n}. \tag{160}$$

As $|H_0 : H_n| = 5^{3n-1}$ for all $n \geq 1$, it follows that $\mathcal{C}_5(X_1(11)/F_\infty)$ has $\Lambda(H_0)$-rank equal to 20.

PROOF. Recalling that it is shown in the previous proof that, in this case, (139) is valid for all $n \geq 1$, we could deduce (160) from Corollary 6.10. However, it is just as easy to argue directly with the fundamental diagram (130) relating $\mathcal{S}_5(X_1(11)/F_\infty)$ to $\mathcal{S}_5(X_1(11)/F_n^{cyc})$ for all $n \geq 0$. Indeed, using the value of $r(n)$ calculated above, we conclude from Lemma 6.7 that, in this case, $\mathrm{Ker}(h)$ has $\boldsymbol{Z}_5$-corank equal to 4 if $n = 0$, and to $4 \times 5^{2n-1}$ if $n \geq 1$. It is then clear that we obtain (160) from (156) using (130). The final assertion then

follows from the well known asymptotic formula (see Lemma 3.4.1 of [**19**], or Theorem 2.22 of [**24**].)

As with Theorem 1.5, we simply do not know whether the $\boldsymbol{Z}_5$-rank in $\mathscr{C}_5(X_1(11)/F_n^{cyc})$ comes from the Mordell-Weil group or the Tate-Shafarevič group of $X_1(11)$ over F_n^{cyc}. Indeed, we want to stress that at present we do not even know if $X_1(11)$ has any points of infinite order in the field F_∞. Of course, Corollary 7.2 shows that $X_1(11)$ has no points of infinite order in $\boldsymbol{Q}(\mu_{5^\infty})$, but this is the limit of our current knowledge. Note that Harris' construction in [**21**] does not apply in this case, since no subgroup of order 11 of $X_1(11)$ is stable under the absolute Galois group of F_n for all $n \geq 0$.

Finally, since the $\boldsymbol{Z}$-rank of $X_1(11)(F_n)$ is bounded above by $\lambda_{inv}(\mathscr{C}_5(X_1(11)/F_n^{cyc}))$, we also obtain the following corollary of Proposition 7.5.

COROLLARY 7.7. *The* $\boldsymbol{Z}$*-rank of* $X_1(11)(F_0)$ *is at most* 16, *and*

$$\boldsymbol{Z}\text{-rank of } X_1(11)(F_n) \leq 4 \times 5^{3n} - 4 \times 5^{2n-1}, \quad n \geq 1. \tag{161}$$

Let $Z = \mathscr{C}_5(X_1(11)/\boldsymbol{Q}(E_{5^\infty}))$. It would be of great interest to explicitly determine the structure of Z as a $\Lambda(H_0)$-module. We know by Corollary 3.8 that Z has no non-zero finite H_0-submodule. We also know that Z has rank 20 over $\Lambda(H_0)$ by Corollary 7.6. In fact, one can prove that Z is not a free $\Lambda(H_0)$-module. On the other hand, one is tempted to speculate that the $\Lambda(H_0)$-torsion submodule of Z is zero. One can even go further and ask whether Z can be embedded in $\Lambda(\Delta)$ with a finite, non-zero cokernel, where $\Delta = \mathrm{Gal}(\boldsymbol{Q}(E_{5^\infty})/\boldsymbol{Q}^{cyc})$.

As is well known (see [**11**]), there are precisely three elliptic curves in the isogeny class of $X_1(11)$. The curve $X_0(11)$ corresponds to the modular group $\Gamma_0(11)$. (It is denoted by 11(A1) in [**11**].) $X_0(11)$ has minimal Weierstraß equation

$$y^2 + y = x^3 - x^2 - 10x - 20 \tag{162}$$

Then the third curve (denoted in [**11**] by 11(A2)) is given by

$$y^2 + y = x^3 - x^2 - 7820x - 263580 \tag{163}$$

Let E^1, E^2 be two elliptic curves defined over a number field, F, and with an F-isogeny

$$\xi : E^1 \to E^2 \tag{164}$$

LEMMA 7.8. $F(E^1_{p^\infty}) = F(E^2_{p^\infty})$

PROOF. Since ξ induces a $\mathrm{Gal}(\bar{F}/F)$-invariant map $E^1_{p^\infty} \to E^2_{p^\infty}$ with finite kernel, it is clear that $F(E^1_{p^\infty})$ is an extension of $F(E^2_{p^\infty})$. The isogeny ξ also

induces maps (denoted $T_p\xi$, $V_p\xi$ respectively) defined by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_pE^1 & \longrightarrow & V_pE^1 & \longrightarrow & E^1_{p^\infty} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle T_p\xi} & & \downarrow{\scriptstyle V_p\xi} & & \downarrow{\scriptstyle \xi} & & \\ 0 & \longrightarrow & T_pE^2 & \longrightarrow & V_pE^2 & \longrightarrow & E^2_{p^\infty} & \longrightarrow & 0 \end{array} \tag{165}$$

Since the right hand map in (165) is surjective, with finite kernel, $V_p\xi$ is an isomorphism and $T_p\xi$ is an injection. Suppose $\sigma \in \mathrm{Gal}(\bar{F}/F(E^2_{p^\infty}))$. Then σ fixes T_pE^2 and thus also the sublattice, T_pE^1. But since

$$E^1_{p^\infty} = \varinjlim T_pE^1/p^nT_pE^1$$

this means $\sigma \in \mathrm{Gal}(\bar{F}/F(E^1_{p^\infty}))$ also. Thus $F(E^2_{p^\infty})$ contains $F(E^1_{p^\infty})$. □

Hence there will be no confusion if we write F_∞ for $F(E^i_{p^\infty})$, and define G_∞ as it has been throughout this paper. We can take R to be defined as in (4) for either curve, E^i. We recall that the reduction type of an elliptic curve is unchanged by isogeny, that is $\tau_p(E^1/F) = \tau_p(E^2/F)$.

PROPOSITION 7.9. *Conjecture* 2.4 *is isogeny invariant. More precisely, if* E^1 *and* E^2 *are isogenous elliptic curves then the compact Selmer groups,* $\mathscr{C}_p(E^1/F_\infty)$ *and* $\mathscr{C}_p(E^2/F_\infty)$, *have the same* $\Lambda(R)$*-ranks.*

PROOF. We have the following diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{S}_p(E^2/F_\infty) & \longrightarrow & H^1(F_\infty, E^2_{p^\infty}) & \longrightarrow & \varinjlim \bigoplus_{\omega_n} H^1(F_{n,\omega_n}, E^2)(p) \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} \\ 0 & \longrightarrow & \mathscr{S}_p(E^1/F_\infty) & \longrightarrow & H^1(F_\infty, E^1_{p^\infty}) & \longrightarrow & \varinjlim \bigoplus_{\omega_n} H^1(F_{n,\omega_n}, E^1)(p) \end{array} \tag{166}$$

the vertical maps being induced by ξ. Since ξ is an *isogeny*, it is a surjection and $\mathrm{Ker}(\xi)$ is a finite group scheme of order $\deg(\xi)$. Let p^t be the maximal power of p dividing $\deg(\xi)$. Then p^t annihilates the kernels and cokernels of the maps g and h. (For example, $\mathrm{Coker}(g)$ embeds into $H^2(F_\infty, \mathrm{Ker}(\xi)(p))$ which is annihilated by $\sharp(\mathrm{Ker}(\xi))$.) It follows that

$$\mathscr{C}_p(E^1/F_\infty) \otimes \boldsymbol{Q}_p \cong \mathscr{C}_p(E^2/F_\infty) \otimes \boldsymbol{Q}_p \tag{167}$$

and the proposition follows. □

Let Ω denote any open subgroup of $\mathrm{Gal}(F_\infty/F^{cyc})$ such that $\Lambda(\Omega)$ has no divisors of zero. Then the proof of Proposition 7.9 shows also that $\mathscr{C}_p(E^1/F_\infty)$

and $\mathscr{C}_p(E^2/F_\infty)$ have the same $\Lambda(\Omega)$-rank, with the understanding that if one is infinite, then both are.

We recall that for $p = 5$, and E either of the two curves (162) or (163) it is well known (see [**10**], [**15**] or [**29**]) that $\mathscr{C}_p(E/\boldsymbol{Q}^{cyc})$ has positive μ-invariant. Hence we deduce the following from Theorem 6.4, Corollary 7.3, Corollary 7.6 and Proposition 7.9.

COROLLARY 7.10. *Take $F = \boldsymbol{Q}$, $p = 5$, and let E be either of the curves* (162) *or* (163). *Let*

$$R = \mathrm{Gal}(\boldsymbol{Q}(E_{5^\infty})/\boldsymbol{Q}(\mu_5)), \quad \Omega = \mathrm{Gal}(\boldsymbol{Q}(E_{5^\infty})/\boldsymbol{Q}(\mu_{5^\infty})). \tag{168}$$

Then:

i) $\mathscr{C}_5(E/\boldsymbol{Q}(E_{5^\infty}))$ *is $\Lambda(R)$-torsion.*

ii) $\mathscr{C}_5(E/\boldsymbol{Q}(E_{5^\infty}))$ *is not a finitely generated $\Lambda(\Omega)$-module.*

iii) $\mathscr{C}_5(E/\boldsymbol{Q}(E_{5^\infty}))$ *has $\Lambda(\Omega)$-rank equal to* 4.

EXAMPLE. Take $E = X_0(11)$. As explained in Greenberg's article [**15**] a 5-decent shows again that

$$Ш(E/\boldsymbol{Q})(5) = 0, \quad E(\boldsymbol{Q}) = \boldsymbol{Z}/5\boldsymbol{Z} \tag{169}$$

We also again have $c_q = 1$ for all $q \neq 11$, but this time

$$c_{11}(E) = 5 \tag{170}$$

The Euler factor at 11 is still given by (152) and we conclude from Theorem 1.1 and Corollary 7.10 that

COROLLARY 7.11. *Let G_∞ be the Galois group of $\boldsymbol{Q}(E_{5^\infty})/\boldsymbol{Q}$ for E the curve $X_0(11)$. Then*

$$\chi(G_\infty, \mathscr{S}_5(X_0(11)/\boldsymbol{Q}(E_{5^\infty}))) = 5^2 \tag{171}$$

Similarly, for E the curve 11(A2) of (163), one can calculate $\chi(G_\infty, \mathscr{S}_5(11(\mathrm{A2})/\boldsymbol{Q}(E_{5^\infty})))$ explicitly.

We first make the following general remark. If $\mathscr{C}_p(E/F^{cyc})$ is not a finitely generated $\boldsymbol{Z}_p$-module, then it is easy to see that, for every finite extension L of F, $\mathscr{C}_p(E/L^{cyc})$ is not a finitely generated $\boldsymbol{Z}_p$-module. However, even if we know that $\mathscr{C}_p(E/F^{cyc})$ is a torsion module over $\Lambda(\Gamma_F)$, (where $\Gamma_F = \mathrm{Gal}(F^{cyc}/F)$) there is no way in general of proving the same is true for $\mathscr{C}_p(E/L^{cyc})$. Notwithstanding that, we do have the following example.

COROLLARY 7.12. *For E either of the curves* (162) *or* (163), $\mathscr{C}_5(E/\boldsymbol{Q}(E_{5^{n+1}})^{cyc})$, *is $\Lambda(\Gamma_n)$-torsion for all $n \geq 0$. It follows that $\mathscr{C}_5(E/\boldsymbol{Q}(E_{5^{n+1}})^{cyc})$ has strictly positive μ-invariant for all $n \geq 0$.*

PROOF. Let $E^0 = X_0(11)$ or $11(A2)$ and $E^1 = X_1(11)$. By Lemma 7.8 $\boldsymbol{Q}(E^0_{5^{n+1}}) \subset \boldsymbol{Q}(E^1_{5^\infty})$. It follows from Theorem 6.4 that $\mathscr{C}_5(E^1/\boldsymbol{Q}(E^0_{5^{n+1}})^{cyc})$ is $\Lambda(\Gamma)$-torsion for $\Gamma = \mathrm{Gal}(\boldsymbol{Q}(E^0_{5^{n+1}})^{cyc}/\boldsymbol{Q}(E^0_{5^{n+1}}))$. Then the same argument as the proof of Proposition 7.9 shows that Conjecture 6.1 is also isogeny invariant. This, together with the remark above, gives the corollary. □

REMARK. In fact one can easily calculate the μ-invariant exactly using the formula given by Perrin-Riou in the appendix to [**34**] (and independently by Schneider in [**35**]) which describes explicitly how the μ-invariant of the Selmer group changes under isogeny. If E_0, E_1 and E_2 denote respectively the curves $X_0(11)$, $X_1(11)$ and 11(A2) then $E_1 = E_0/\mu_5$, $E_2 = E_0/(\boldsymbol{Z}/5\boldsymbol{Z})$. Let μ_{inv} denote the μ-invariant of a finitely generated, torsion $\Lambda(\Gamma)$-module. Then

COROLLARY 7.13. *Let L denote any finite extension of $\boldsymbol{Q}(\mu_5)$ contained in $\boldsymbol{Q}(E_{5^\infty})$, where E is any of E_0, E_1 or E_2 (recall $\boldsymbol{Q}(E_{5^\infty})$ is the same field for all). Then*

$$\mu_{inv}(\mathscr{S}_5(E_0/L^{cyc})) = \frac{1}{2}|L:\boldsymbol{Q}| \tag{172}$$

$$\mu_{inv}(\mathscr{S}_5(E_2/L^{cyc})) = |L:\boldsymbol{Q}| \tag{173}$$

We finish with the following observation, which is a well known consequence of Corollary 7.12.

COROLLARY 7.14. *Let E be any of the three curves of conductor* 11. *Let L be any finite extension of $\boldsymbol{Q}$ contained in $\boldsymbol{Q}(E_{5^\infty})$. Then, $E(L(\mu_{5^\infty}))$ is finitely generated as an Abelian group.*

We recall that so far we cannot exhibit a single non-torsion element in $E(L(\mu_{5^\infty}))$ for L any finite extension of $\boldsymbol{Q}$ contained in $\boldsymbol{Q}(E_{5^\infty})$.

Appendix. Proof of theorem 1.5.

We are most grateful to R. Greenberg for giving us the essential ideas behind this proof.

We assume $p \geq 5$ throughout this appendix, although this is not necessary if E has non-integral j-invariant at any prime of F dividing p. We need one extra piece of notation. Denote by Σ_n the Galois group $\mathrm{Gal}(F_\infty/F_{n+1})$, so $G_\infty/\Sigma_n = G_n$. We use the term 'ordinary reduction' to mean either good ordinary or split multiplicative reduction.

The first thing to note is that the conclusion of Theorem 1.5 is trivially true if $\mathscr{C}_p(E/F_\infty)$ is not a torsion $\Lambda(R)$-module and so, from now until the end, we assume that this is the case. But from Theorem 2.5 we know that this means

that E has either potential good ordinary reduction or non-integral j-invariant at all primes of F above p. We now give the proof of Theorem 1.5 under this assumption.

LEMMA A.1. *Let v be either any prime of F dividing p such that E has potential ordinary reduction at v or any prime of F such that $ord_v(j_E) < 0$. Then the number of primes of F_n lying above v is unbounded, as n tends to infinity.*

PROOF. We saw in §5 (Lemma 5.1) that for any $\omega|v$ the decomposition group, Δ_ω, of ω in the extension F_∞/F, is a p-adic Lie group of dimension at most 3 for v satisfying either of the conditions of the lemma. Since G_∞ has dimension 4 as a p-adic Lie group, the lemma follows. □

Then we can give a simple proof of Theorem 1.5 under the condition that there is at least one prime v of F_0 at which E has split multiplicative reduction. We do not even need to assume that $v|p$. Taking $L = F_n$ and $H_n = \mathrm{Gal}(F_\infty/F_n)$ in diagram (130) we know from the finiteness of $H^1(H_n, E_{p^\infty})$ that the restriction map

$$f_n : \mathcal{S}_p(E/F_n^{cyc}) \to \mathcal{S}_p(E/F_\infty)^{H_n} \tag{174}$$

has finite kernel. It follows that Theorem 1.5 is clear if there exists some $n \geq 0$ such that $\mathcal{C}_p(E/F_n^{cyc})$ is not $\Lambda(\Gamma_n)$-torsion, where we recall $\Gamma_n = \mathrm{Gal}(F_n^{cyc}/F_n)$. Hence we assume that $\mathcal{C}_p(E/F_n^{cyc})$ is $\Lambda(\Gamma_n)$-torsion, for all $n \geq 0$. Thus, from Proposition 6.2, the bottom, right hand, horizontal map in (130) is a surjection. By the snake lemma applied to that diagram, together with Lemma 6.7

$$\boldsymbol{Z}_p\text{-corank}(\mathrm{Coker}(f_n)) = \boldsymbol{Z}_p\text{-corank}(\mathrm{Ker}(h_n)), \tag{175}$$

where h_n denotes the right hand, vertical map in (130) for $L = F_n$. But under our assumption that E has split multiplicative reduction at v, in view of Lemma 5.28 if $v|p$ and Lemma 5.13 if $v \nmid p$, together with Lemma A.1, we see that the right hand side of (175) is unbounded as $n \to \infty$, proving Theorem 1.5 in this case.

But, by Lemma 5.29, if v is a prime of F dividing p such that $ord_v(j_E) < 0$ then E has split multiplicative reduction at all primes of F_0 dividing v. Thus we may assume E has potential good reduction at all primes v of F dividing p. Furthermore, by the above remark we may assume E has potential good *ordinary* reduction at v and we make this assumption throughout the remainder. (We need no condition on the primes not dividing p for this argument.)

First, suppose that the $\boldsymbol{Z}_p$-corank of $\mathcal{S}_p(E/F_n)$ is unbounded as $n \to \infty$. We saw above, in Theorem 2.9, that the map

$$\mathcal{S}_p(E/F_n) \to \mathcal{S}_p(E/F_\infty)^{\Sigma_n} \tag{176}$$

induced by the restriction map has finite kernel. So $\mathcal{S}_p(E/F_\infty)$ contains arbitrarily many copies of $\boldsymbol{Q}_p/\boldsymbol{Z}_p$, and Theorem 1.5 follows in this case.

Thus we may assume that the $\boldsymbol{Z}_p$-corank of $\mathcal{S}_p(E/F_n)$ is bounded as n grows. Consider the following commutative diagram, which is simply (16) with the ground field, F, replaced by F_n:

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathcal{S}_p(E/F_\infty)^{\Sigma_n} & \longrightarrow & H^1(F_S/F_\infty, E_{p^\infty})^{\Sigma_n} & \xrightarrow{\psi_n} & \left(\bigoplus_{\omega_n|S} J_{\omega_n}(F_\infty)\right)^{\Sigma_n} & \\ & \uparrow{\scriptstyle \alpha_n} & & \uparrow{\scriptstyle \beta_n} & & \uparrow{\scriptstyle \delta_n} & \\ 0 \longrightarrow & \mathcal{S}_p(E/F_n) & \longrightarrow & H^1(F_S/F_n, E_{p^\infty}) & \xrightarrow{\lambda_n} & \bigoplus_{\omega_n|S} H^1(F_{n,\omega_n}, E)(p), & \end{array} \tag{177}$$

Here we define

$$J_{\omega_n}(F_\infty) = \varinjlim_m \bigoplus_{\varpi|\omega_n} H^1(F_{m,\varpi}, E)(p), \tag{178}$$

exactly as in (15) above.

First consider $\ker(\beta_n) = H^1(\Sigma_n, E_{p^\infty})$. By Lemma 4.1, this is known to be finite. However, Greenberg has analysed it more closely and proves the following in [**14**].

LEMMA A.2. *For $n \gg 0$*

$$\mathrm{Ker}(\beta_n) \cong (\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^6 \tag{179}$$

as an Abelian group.

PROOF. We will not give all the details. The idea is that for $n \gg 0$ the centre of Σ_n consists of just the scalar matrices congruent to 1 modulo p^{n+1}, and then $H^1(F_\infty/F_n, E_{p^\infty}) = H^1(P, E_{p^{n+1}})$, where P is the quotient of Σ_n by its centre. This is a p-adic Lie group of dimension 3 which, for $n \gg 0$, is uniform and thus satisfies

$$P/[P,P]P^{p^{n+1}} \cong (\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^3. \tag{180}$$

But P acts trivially on $E_{p^{n+1}}$ and so $H^1(P, E_{p^{n+1}})$ is just the group $\mathrm{Hom}(P, E_{p^{n+1}})$. Since $E_{p^{n+1}}$ is isomorphic to $\boldsymbol{Z}/p^{n+1}\boldsymbol{Z}$ as an Abelian group, the lemma follows. □

Now we look at the local restriction maps. Let $\Delta_{n,\omega}$ denote $\mathrm{Gal}(F_{\infty,\omega}/F_{n,\omega_n})$. Recall that, as in (19),

$$\mathrm{Ker}(\delta_n) = \bigoplus_{\omega_n|S} H^1(\Delta_{n,\omega}, E(F_{\infty,\omega}))(p). \tag{181}$$

Since we are assuming that ω_n is a prime for which E has potential good ordinary reduction, as we saw in 5.20 above, as an Abelian group $H^1(\Delta_{n,\omega}, E(F_{\infty,\omega}))(p)$ contains the cyclic subgroup which was there denoted by $\mathfrak{F}(E(F_{n,\omega_n}))(p)$. For n sufficiently large this is isomorphic to $\boldsymbol{Z}/p^{n+1}\boldsymbol{Z}$ as an Abelian group. So we obtain the following, exact as a sequence of Abelian groups

$$0 \to \boldsymbol{Z}/p^{n+1}\boldsymbol{Z} \to H^1(F_{\infty,\omega}/F_{n,\omega_n}, E), \tag{182}$$

and so, again exact as a sequence of Abelian groups, we have

$$0 \to (\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^{r(n)} \to \mathrm{Ker}(\delta_n), \tag{183}$$

where $r(n)$ equals the number of primes of F_n dividing v and so $r(n) \to \infty$, as $n \to \infty$, by Lemma A.1 above.

Recall, (39), how the Cassels-Poitou-Tate sequence describes the cokernel of the map λ_n in diagram (177).

$$0 \to \mathrm{Coker}(\lambda_n) \to \widehat{\mathscr{R}_p(E/F_n)} \tag{184}$$

where $\mathscr{R}_p(E/F_n)$ is the *compact* Selmer group defined as in (40). It sits in the exact sequence

$$0 \to E(F_n) \hat{\otimes} \boldsymbol{Z}_p \to \mathscr{R}_p(E/F_n) \to T_p Ш(E/F_n) \to 0. \tag{185}$$

Since we are assuming the $\boldsymbol{Z}_p$-corank of $\mathscr{S}_p(E/F_n)$ is bounded, as $n \to \infty$, this implies the $\boldsymbol{Z}_p$-corank of $Ш(E/F_n)(p)$ is bounded as $n \to \infty$ and so

$$T_p Ш(E/F_n) \cong \boldsymbol{Z}_p^N, \quad \text{for } n \gg 0 \tag{186}$$

for some N, independent of n. Similarly, the $\boldsymbol{Z}_p$-rank of $E(F_n) \hat{\otimes} \boldsymbol{Z}_p$ is a fixed constant, M say, for $n \gg 0$. It follows that

$$E(F_n) \hat{\otimes} \boldsymbol{Z}_p \cong \boldsymbol{Z}_p^M \oplus E_{p^{n+1}}, \quad n \gg 0. \tag{187}$$

By (184) this implies that, as Abelian groups,

$$\mathrm{Coker}(\lambda_n) \hookrightarrow \widehat{\mathscr{R}_p(E/F_n)} \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^R \oplus (\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^2, \tag{188}$$

where R is independent of n.

Recalling the basic diagram (177) above, the snake lemma gives the exact sequence

$$\mathrm{Ker}(\beta_n) \to \mathrm{Ker}(\delta_n) \cap \mathrm{im}(\lambda_n) \to \mathrm{Coker}(\alpha_n) \tag{189}$$

Consider, now, the following variant of diagram (27) above:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{im}(\psi_n) & \longrightarrow & \left(\bigoplus_{\omega_n|S} J_{\omega_n}(F_\infty)\right)^{\Sigma_n} & \longrightarrow & \mathrm{Coker}(\lambda_\infty) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow{\scriptstyle \delta_n} & & \uparrow & & \\
0 & \longrightarrow & \mathrm{im}(\lambda_n) & \longrightarrow & \bigoplus_{\omega_n|S} H^1(F_{n,\omega_n}, E)(p) & \longrightarrow & \mathrm{Coker}(\lambda_n) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \mathrm{Ker}(\delta_n) \cap \mathrm{im}(\lambda_n) & & \mathrm{Ker}(\delta_n) & & X_n & &
\end{array} \tag{190}$$

where X_n is defined to be the kernel of the right hand vertical map. This gives rise to

$$0 \to \mathrm{Ker}(\delta_n) \cap \mathrm{im}(\lambda_n) \to \mathrm{Ker}(\delta_n) \to X_n \tag{191}$$

where

$$X_n \hookrightarrow \mathrm{Coker}(\lambda_n) \hookrightarrow (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^R \oplus (\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^2 \tag{192}$$

from (188), above and so the number of $\boldsymbol{Z}_p$-cogenerators of X_n is bounded, independently of n. But we know, from the local result (183), that $\mathrm{Ker}(\delta_v)$ contains the Abelian subgroup $(\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^{r(n)}$, with $r(n)$ unbounded as $n \to \infty$. It follows that for n sufficiently large we must have

$$(\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^{r'(n)} \hookrightarrow \mathrm{Ker}(\delta_n) \cap \mathrm{im}(\lambda_n) \tag{193}$$

where $r'(n)$ is also unbounded as $n \to \infty$.

This information, (193), together with the sequence (189) and Lemma A.2 describing the behaviour of $\mathrm{Ker}(\beta_n)$ then implies that

$$(\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^{r''(n)} \hookrightarrow \mathrm{Coker}(\alpha_n). \tag{194}$$

Here $r''(n)$ again is unbounded as $n \to \infty$. So, as Abelian groups, for n sufficiently large we have

$$\begin{array}{ccccccc}
\mathscr{S}_p(E/F_n) & \longrightarrow & \mathscr{S}_p(E/F_\infty)^{\Sigma_n} & \longrightarrow & \mathrm{Coker}(\alpha_n) & \longrightarrow & 0 \\
 & & & & \uparrow & & \\
 & & & & (\boldsymbol{Z}/p^{n+1}\boldsymbol{Z})^{r''(n)} & & \\
 & & & & \uparrow & & \\
 & & & & 0 & &
\end{array} \tag{195}$$

and $r''(n)$ is unbounded. Thus it follows that $\mathcal{S}_p(E/F_\infty)$ requires infinitely many $\boldsymbol{Z}_p$-cogenerators. But this is not quite strong enough. Theorem 1.5 follows immediately, however, from (195) and the following general lemma about the structure of finitely generated $\Lambda(R)$-modules.

LEMMA A.3. *Let M be any finitely generated (left or right) $\Lambda(R)$-module. Then the exponent of the submodule, $M(p)$, comprising all the p-torsion in M, is finite.*

Note that because the action of $\boldsymbol{Z}_p$ commutes with that of R, $M(p)$ really is a $\Lambda(R)$-submodule of M.

PROOF. Recall from 2.3 that $\Lambda(R)$ is a (left or right, we shall omit this) Noetherian ring. Thus a $\Lambda(R)$-module is finitely generated if and only if it is itself Noetherian. Also, submodules of Noetherian modules are themselves Noetherian. Thus $M(p)$ is Noetherian and so finitely generated as a $\Lambda(R)$-module. Suppose it is generated by $\{x_1, x_2, \ldots, x_r\}$. Then there is some finite integer, t say, such that p^t annihilates all the x_i. But then, since the x_i form a generating set for $M(p)$, and since p commutes with all the elements of R, it follows that p^t annihilates $M(p)$. □

Thus we see that the cogenerators of $\mathcal{S}_p(E/F_\infty)$, whose existence is implied by diagram (195), must actually generate infinitely many copies of $\boldsymbol{Z}_p$ in $\mathcal{C}_p(E/F_\infty)$. □

References

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

[2] K. Barré-Sirieix, G. Diaz, F. Gramain, and G. Philibert, Une Preuve de la Conjecture de Mahler-Manin, Invent. Math., **124** (1996), 1–9.

[3] J. W. S. Cassels and A. Fröhlich, editors, Algebraic Number Theory, Academic Press, 1967.

[4] J. H. Coates, Fragments of the GL_2 Iwasawa Theory of Elliptic Curves without Complex Multiplication, Number 1716 in LNM, Springer, 1999, 1–50.

[5] J. H. Coates, and R. Greenberg, Kummer Theory for Abelian Varieties over Local Fields, Invent. Math., **124**(1–3) (1996), 129–174.

[6] J. H. Coates, R. Greenberg, B. Mazur, and I. Satake, editors, Algebraic Number Theory, Number 17 in Adv. Stud. Pure Math. Academic Press Inc., Boston, Mass., 1989. Papers in honour of K. Iwasawa on the occasion of his 70th birthday.

[7] J. H. Coates and S. Howson, Euler Characteristics and Elliptic Curves, Proc. Nat. Acad. Sci. U.S.A., **94**(21) (1997), 11115–11117.

[8] J. H. Coates and G. McConnell, Iwasawa Theory of Modular Elliptic Curves of Analytic Rank at most 1, J. London Math. Soc. (2), **50**(2) (1994), 243–264.

[9] J. H. Coates and R. Sujatha, Euler-Poincaré Characteristics of Abelian Varieties, C. R. Acad. Sci. Paris, t. 329 (1999), 309–313.

[10] J. H. Coates and R. Sujatha, Galois Cohomology of Elliptic Curves, Lecture Notes at the Tata Institute of Fundamental Research No. 88, Narosa, 2000.

[11] J. Cremona, Algorithms for Modular Elliptic Curves, C.U.P., second edition, 1997.
[12] D. Delbourgo, Non-Archimedean L-Series at Non-Ordinary Primes, PhD thesis, University of Cambridge, 1997.
[13] K. R. Goodearl and R. B. Warfield, An Introduction to Noncommutative Noetherian Rings, Number 16 in L.M.S. Student Texts. C.U.P., Cambridge, 1989.
[14] R. Greenberg, Galois Theory for the Selmer Group of an Abelian Variety, preprint.
[15] R. Greenberg, Iwasawa Theory of Elliptic Curves, Number 1716 in LNM, Springer, 1999, 51–144.
[16] R. Greenberg, Iwasawa Theory of p-adic Representations, In Algebraic Number Theory, pages 97–137. See [6].
[17] R. Greenberg, The Structure of Selmer Groups, Proc. Natl. Acad. Sci., **94**(21) (1997), 11125–11128.
[18] Y. Hachimori and K. Matsuno, An Analogue of Kida's Formula for the Selmer Group of Elliptic Curves, J. Algebraic Geom., **8** (1999), 581–601.
[19] M. Harris, p-adic Representations Arising from Descent on Abelian Varieties, PhD thesis, Harvard, 1977.
[20] M. Harris, p-adic Representations Arising from Descent on Abelian Varieties, Compositio Math., **39**(2) (1979), 177–245.
[21] M. Harris, Systematic Growth of Mordell-Weil Groups of Abelian Varieties in Towers of Number Fields, Invent. Math., **51**(2) (1979), 123–141.
[22] M. Harris, Correction to "p-adic Representations Arising from Descent on Abelian Varieties", to appear in Compositio Math., 1998.
[23] G. P. Hochschild and J-P. Serre, Cohomology of Group Extensions, Trans. A.M.S., 1953.
[24] S. Howson, Iwasawa Theory of Elliptic Curves for p-adic Lie Extensions, PhD thesis, University of Cambridge, 1998.
[25] S. Howson and Y-H. Ochi, Structure of Iwasawa–Modules Arising from Galois Cohomology, in preparation.
[26] K. Kato, p-adic Hodge Theory and Values of Zeta Functions of Modular Forms, preprint.
[27] S. Lang and H. Trotter, Frobenius Distributions in GL_2-extensions: Distribution of Frobenius automorphisms in G_2-extensions of the rational numbers, Number 504 in LNM. Springer, 1976.
[28] M. Lazard, Groupes Analytiques p-adiques, Publ. Inst. Hautes Études Scientifiques, **26** (1965), 389–603.
[29] B. Mazur, Rational Points of Abelian Varieties with Values in Towers of Number Fields, Invent. Math., **18** (1972), 183–266.
[30] B. Mazur, J. Tate, and Teitelbaum, On the p-adic Analogues of the Conjectures of Birch and Swinnerton-Dyer, Invent. Math., **84** (1986), 1–48.
[31] J. S. Milne, Arithmetic Duality Theorems, Perspectives in Mathematics. Academic Press, Boston, Mass., 1986.
[32] Y-H. Ochi, Iwasawa Modules Via Homotopy Theory, PhD thesis, University of Cambridge, 1999.
[33] B. Perrin-Riou, Arithmétique des Courbes Elliptiques et Théorie d'Iwasawa, Mém. Soc. Math. France, **17** (1984), 1–130.
[34] B. Perrin-Riou, Fonctions L p-adiques, Théorie d'Iwasawa et Points de Heegner, Bull. Soc. Math. France, **115**(4) (1987), 399–456.
[35] P. Schneider, The μ-invariant of Isogenies, J. Indian Math. Soc. (N.S.), **52** (1987), 159–170.
[36] A. J. Scholl and R. L. Taylor, editors, Galois Representations in Arithmetic and Geometry, L.M.S., C.U.P., 1998.
[37] J-P. Serre, Sur les Groupes de Congruence des Variétés Abéliennes I, Izv. Acad. Nauk. SSSR, **28** (1964), 3–18.
[38] J-P. Serre, Sur la Dimension Cohomologique des Groupes Profinis, Topology, **3** (1965), 413–420.
[39] J-P. Serre, Abelian l-adic Representations and Elliptic Curves, W. A. Benjamin, 1968.

[40] J-P. Serre, Sur les Groupes de Congruence des Variétés Abéliennes II, Izv. Acad. Nauk. SSSR, **35** (1971), 731–735.
[41] J-P. Serre, Propriétés Galoisiennes des Points d'ordre Fini des Courbes Elliptiques, Invent. Math., **15** (1972), 259–331.
[42] J-P. Serre, Local Fields, Number 67 in G.T.M. Springer, 1979.
[43] J-P. Serre, Cohomologie Galoisienne, Number 5 in LNM. Springer, fifth edition, 1994.
[44] J-P. Serre, La Distribution d'Euler-Poincaré d'un Groupe Profini, In Galois Representations in Arithmetic and Geometry, 1998. See [36].
[45] J-P. Serre and J. Tate, Good Reduction of Abelian Varieties, Annals of Maths., **88** (1968), 492–517.
[46] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Number 151 in GTM. Springer, 1994.

John COATES
D.P.M.M.S.
Centre for Mathematical Sciences
Wilberforce Road
Cambridge
CB3 0WB
England
E-mail: J.H.Coates@dpmms.cam.ac.uk

Susan HOWSON
School of Mathematical Sciences
University Park
Nottingham
NG7 2RD
England
E-mail: Susan.Howson@maths.nottingham.ac.uk