COMPOSITIO MATHEMATICA

GARY MCCONNELL

On the Iwasawa theory of CM elliptic curves at supersingular primes

Compositio Mathematica, tome 101, nº 1 (1996), p. 1-19

<http://www.numdam.org/item?id=CM_1996__101_1_1_0>

Compositio Mathematica **101:** 1–19, 1996.
© 1996 *Kluwer Academic Publishers. Printed in the Netherlands.*

On the Iwasawa theory of CM elliptic curves at supersingular primes

GARY McCONNELL*
Mathematisches Institut, Westfälische Wilhelms-Universität, Einsteinstrasse 62, 48149 Münster, Germany

Received 13 December 1994; accepted in final form 22 December 1994

1. Introduction and statement of results

Let K be a number field, and let E be an elliptic curve defined over K. Let p be any odd prime, and let K_∞^c be the cyclotomic $\mathbb{Z}_p$-extension of K with galois group Γ_c and Iwasawa algebra

$$\Lambda_c = \mathbb{Z}_p[[\Gamma_c]],$$

the completion of the $\mathbb{Z}_p$-group ring of Γ_c with respect to the topology defined by its maximal ideal. We may also identify Λ_c with the formal power series ring in one variable over $\mathbb{Z}_p$, the identification being realised (non-canonically) by sending a choice of topological generator γ for Γ_c, to the polynomial $(1+T)$. Using Tate's notion of global Euler-Poincaré characteristics, Schneider [Sc] and Greenberg [Gr3] have formulated conjectures on the Λ_c-corank of certain Selmer groups attached to E over K_∞^c. Numerous special cases of these conjectures have been proved (see below). In this paper we prove another, namely when K is an imaginary quadratic field over which E has complex multiplication and p is a prime where E has good supersingular reduction.

In a forthcoming joint paper with Rod Yager [McY] we extend these results, obtaining some interesting connections between the modules considered in this paper and special values of L-functions attached to E.

1.1. Statement of the main theorem

We fix some notation which will be standard throughout the paper. Given an odd rational prime p, write E_{p^∞} for the union over all $m \geqslant 1$ of the p^m-torsion points E_{p^m} of E. For any number field K, let K_n^c denote the n-th level of the cyclotomic $\mathbb{Z}_p$-extension K_∞^c of K, so $\mathrm{Gal}(K_n^c|K) \cong \mathbb{Z}/p^n\mathbb{Z}$. Let Σ be a finite set of places of K containing the primes above p, the archimedean prime and the primes where

* Current address: 4/40-42 William IV St. Covent Garden London WC2N 4DD England.

E has bad reduction. We denote by K_Σ the maximal Galois extension of K which is unramified outside the primes in Σ. Write $G_{\infty,\Sigma}$ for the galois group of K_Σ over K^c_∞, and $G_{n,\Sigma}$ for the galois group of K_Σ over K^c_n. For any galois group $G, H^i(G, M)$ will denote the i-th galois cohomology group of the $\mathbb{Z}_p[G]$-module M. We shall also use properties of *continuous* galois cohomology as defined in [Ta].

CONJECTURE 1 (Schneider/Greenberg). *Let E be an elliptic curve defined over the number field K and let p be any odd prime. Then*

$$H^2(G_{\infty,\Sigma}, E_{p^\infty}) = (0).$$

For a more general statement of this conjecture the reader is referred to [Gr3]. The known results are as follows. Suppose first that $K = \mathbb{Q}$ and E is modular. Define the *analytic rank* $r_{a,E}$ of E to be the order of vanishing of the complex L-function attached to E at $s = 1$. Using deep results of Kolyvagin [Ko] it is shown in [CMc] that if $r_{a,E} \leqslant 1$ then indeed conjecture 1 holds for all odd primes p. The only other instances where the conjecture has been demonstrated are where E has complex multiplication. So we specialize now to the case where K is an imaginary quadratic field and E has complex multiplication by the ring of integers $\mathcal{O}_K$ of K. Rubin [Ru3, 4.4] has shown that if E is defined over $\mathbb{Q}$ and $p > 2$ is a prime of good ordinary reduction for E, then the conjecture is true for E at p. Further, in the discussion after that theorem he extends his result to more general cases (including where E is defined over the field of complex multiplication).

Our main result is the following.

THEOREM 1. *Let K be an imaginary quadratic field. Let E be an elliptic curve defined over K with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. Let $\mathfrak{p}$ be a prime of K lying above p which is coprime to the number w_K of roots of unity in K, and suppose that E has good, supersingular reduction at* $\mathfrak{p}$. *Then*

$$H^2(G_{\infty,\Sigma}, E_{p^\infty}) = (0).$$

REMARKS. (1) Our hypotheses imply that p is inert or ramified in $K : \mathbb{Q}$ and that K has class number one (see for example [G, Sect. 5.1]). Furthermore, the stipulation that p be coprime to w_K only excludes the case $K = \mathbb{Q}(\sqrt{-3})$ and $p = 3$. So apart from this case, it is now known that when E is defined over an imaginary quadratic field K over whose ring of integers it has complex multiplication, conjecture 1 holds for all primes $\mathfrak{p} \nmid 2$ of good reduction.

(2) The proof extends in an obvious fashion to any curve E with complex multiplication defined over a number field F satisfying Shimura's condition that the field $F(E_{\text{tors}})$ obtained by adjoining to F the coordinates of *all* torsion points of E, is an abelian extension *of* K. We have omitted the details of such a generalisation

for the sake of clarity of exposition; for the necessary framework we refer the reader to [Ru1].

The proof of Theorem 1 proceeds in a manner similar to Rubin's proof in the ordinary case [Ru3, 4.4], using a deep analytic result of Rohrlich [Ro] on the non-vanishing of special values of modular L-functions twisted by Dirichlet characters. The crucial ingredient is Rubin's supersingular analogue of the Coates–Wiles 'main conjecture of Iwasawa theory' for imaginary quadratic fields [Ru4], which enables us to translate the problem on elliptic curves into a problem on elliptic units. The Coates–Wiles logarithmic derivative homomorphism then links the elliptic units to special values of L-functions.

1.2. Notation

In order to simplify the presentation, for the remainder of Section 1 and all of Section 2 we work under the hypothesis, except where otherwise indicated, that E is defined over $\mathbb{Q}$. The concepts necessary for a generalisation to arbitrary number fields of what is said in this and the next section are essentially explained in [Gr3] and [P-R2].

Fix an odd rational prime p. If A is any abelian group, $\hat{A}$ (or sometimes $A^\wedge$) will denote the Pontrjagin dual of A, and A^{*p} its p-adic completion. The (p-adic) Tate module $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, A)$ of A will be denoted by $T_p(A)$. When $A = E_{p^\infty}$ we just write T_pE. Let $t_{\mathbb{Z}_p}(A)$ denote the maximal $\mathbb{Z}_p$-torsion subgroup of A. From now on we shall write D_p for the divisible group $\mathbb{Q}_p/\mathbb{Z}_p$. If G is any group and M any G-module then M^G will denote the *G-invariants* of M, the maximal G-submodule of M which is (pointwise!) fixed under the action of G. Similarly, we define the group of *G-coinvariants* of M to be the maximal quotient module M_G of M which is pointwise fixed under the action of G.

1.2.1. *Galois cohomology groups*

Let $n \in \mathbb{N} \cup \{0, \infty\}$. The prime p is totally ramified in the extension $\mathbb{Q}^c_\infty : \mathbb{Q}$ and so we shall just write p for the unique prime above p of any subfield $\mathbb{Q}^c_{n,p}$. Define for $i = 1, 2$:

$$X^i_{n,\Sigma} = H^i(G_{n,\Sigma}, E_{p^\infty})^\wedge,$$

where $X^i_{\infty,\Sigma}$ is understood to be the Pontrjagin dual of the inductive limit with respect to the restriction maps in galois cohomology of the modules $H^i(G_{n,\Sigma}, E_{p^\infty})$. Next, we define the continuous cohomology modules:

$$\check{X}^i_{n,\Sigma} = H^i(G_{n,\Sigma}, T_pE)$$

for n finite; when $n = \infty$ we take the projective limit with respect to the norm (corestriction) maps to obtain $\check{X}^i_{\infty,\Sigma}$.

By Tate local duality and the Weil pairing (see [Mi, I]) for every place v and every pair $0 \leqslant n, m < \infty$ we have

$$H^1(\mathbb{Q}^c_{n,v}, E_{p^m}) \cong H^1(\mathbb{Q}^c_{n,v}, E_{p^m})^\wedge$$

and so it follows that for all $n \geqslant 0$:

$$X^1_{n,p} \overset{\mathrm{def}}{=} H^1(\mathbb{Q}^c_{n,p}, E_{p^\infty})^\wedge = H^1(\mathbb{Q}^c_{n,p}, T_pE) \tag{1}$$

and for v any place *not* dividing p:

$$\begin{aligned} X^1_{n,v} &\overset{\mathrm{def}}{=} H^1(\mathbb{Q}^c_{n,v}, E_{p^\infty})^\wedge = H^1(\mathbb{Q}^c_{n,v}, T_pE) = E(\mathbb{Q}^c_{n,v})^{*p} \\ &= H^1(\mathbb{Q}^c_{n,v}, E)(p)^\wedge, \end{aligned} \tag{2}$$

the last two equalities following from Kummer theory, since for v prime to p:

$$E(\mathbb{Q}^c_{n,v}) \otimes_{\mathbb{Z}_p} D_p{}^\wedge = T_p(H^1(\mathbb{Q}^c_{n,v}, E)) = (0).$$

For $n = \infty$ we take the obvious projective limits with respect to the norm (corestriction) maps.

It is easy to show using Nakayama's lemma that each of the modules defined above is a compact finitely-generated Λ_c-module. The structure theory of such modules was developed by Iwasawa; see [Bo, VII] for a general exposition. We define the *rank* of a Λ_c-module M to be the $\mathcal{F}_{\Lambda_c}$-dimension of $M \otimes_{\Lambda_c} \mathcal{F}_{\Lambda_c}$, where $\mathcal{F}_{\Lambda_c}$ denotes the field of fractions of Λ_c. Dually, if M is a discrete Λ_c-module the Λ_c-*corank* will mean the Λ_c-rank of $\hat{M}$.

1.2.2. *Selmer groups*

Let L be any extension of $\mathbb{Q}$ contained in $\mathbb{Q}_\Sigma$. Define the p^m-Selmer group $S^{p^m}_{E|L}$ of E over L by the exactness of the sequence

$$0 \to S^{p^m}_{E|L} \to H^1(G_{L,\Sigma}, E_{p^m}) \to \oplus_{v|\Sigma} H^1(L_v, E)_{p^m},$$

and the so-called 'modified' p^m-Selmer group $S'^{p^m}_{E|L}$ by the exactness of

$$0 \to S'^{p^m}_{E|L} \to H^1(G_{L,\Sigma}, E_{p^m}) \to \oplus_{v|\Sigma\setminus\{p\}} H^1(L_v, E)_{p^m}. \tag{3}$$

We further define an 'unramified' p^m-Selmer group via the exactness of

$$0 \to R^{p^m}_{E|L} \to S^{p^m}_{E|L} \to \oplus_{\mathfrak{p}|p} H^1(L_\mathfrak{p}, E_{p^m}). \tag{4}$$

Taking inductive limits with respect to the maps on cohomology induced by the inclusion maps $E_{p^m} \hookrightarrow E_{p^{m+1}}$ gives the (p^∞)-Selmer groups

$$S_{E|L}, S'_{E|L} \quad \text{and} \quad R_{E|L},$$

and taking projective limits with respect to the maps on cohomology induced by the multiplication by p maps $p\colon E_{p^{m+1}} \to E_{p^m}$ we get the 'continuous' Selmer groups:

$$\check{S}_{E|L}, \check{S}'_{E|L} \quad \text{and} \quad \check{R}_{E|L}.$$

When $L = \mathbb{Q}_n^c$ for some $n, 0 \leqslant n \leqslant \infty$, we shall denote these modules simply by

$$S_n, \quad S'_n, \quad R_n, \quad \check{S}_n, \quad \check{S}'_n, \quad \check{R}_n$$

respectively.

It is easy to show that when $L = \mathbb{Q}_\infty^c$, the groups $\widehat{S_\infty}, \widehat{S'_\infty}, \widehat{R_\infty}, \check{S}_\infty, \check{S}'_\infty$ and $\check{R}_\infty$ are naturally compact finitely-generated Λ_c-modules. We shall use this fact without further comment in the sequel.

2. Reduction to a problem on R_∞

Conjecture 1 has been investigated in a number of guises and it is not always apparent how they interrelate. The following theorem explains some of these connections. Here in the statement of the theorem we allow ourselves the freedom that K be an arbitrary number field.

THEOREM 2. *Let E be an elliptic curve defined over a number field K of absolute degree δ_K. Let p be any odd prime. The following statements are equivalent:*

(i) $X^1_{\infty,\Sigma}$ *has* Λ_c-*rank* δ_K*;*
(ii) $X^2_{\infty,\Sigma}$ *is* Λ_c-*torsion;*
(iii) $X^2_{\infty,\Sigma} = (0)$*;*
(iv) $\widehat{S'_\infty}$ *has* Λ_c-*rank* δ_K*;*
(v) $\check{R}_\infty$ *is* Λ_c-*torsion;*
(vi) $\check{R}_\infty = (0)$*;*
(vii) $\widehat{R_\infty}$ *is* Λ_c-*torsion;*
(viii) $\check{X}^2_{\infty,\Sigma}$ *is* Λ_c-*torsion;*
(ix) $\check{X}^1_{\infty,\Sigma}$ *has* Λ_c-*rank* δ_K.

Moreover, when p is a prime of (potentially) supersingular reduction for E, the above statements are equivalent to

(x) $\check{S}_\infty = (0)$.

REMARKS. (1) In a forthcoming note [Mc2] we shall show that if E is defined over $\mathbb{Q}$ and p is a prime of good ordinary reduction for E, statements (i)–(ix) are *equivalent* to the conjecture of Mazur that $\widehat{S_\infty}$ should be a Λ_c-torsion Λ_c-module. (Equivalently again, that $\check{S}_\infty = (0)$). That this conjecture implies the above statements is easy to deduce from the definitions; the reverse implication requires recent deep results of Kato (soon to be published). It should also be mentioned here that the module for which Kato formulates his 'Iwasawa main conjecture' is the one defined as $\check{X}^2_{\infty,\Sigma}$ above. See also [CMc].

(2) As a consequence of remark(1) it follows from [CMc, Theorem 1] that if E is a modular elliptic curve of analytic rank 1 and if p is a prime of good ordinary reduction for E then in fact $\widehat{S_\infty}$ is Λ_c-torsion. This was previously only known in the cases when E is modular of analytic rank zero (Kolyvagin [Ko]) and when E has complex multiplication (Rubin [Ru3, Sect. 4]).

(3) Greenberg [Gr3, Proposition 5] has shown that if any of the above statements holds then $X^1_{\infty,\Sigma}$ has no non-zero finite submodules. As a corollary, it is easy to show using forthcoming results of Coates and Greenberg [CGr] that $\widehat{S'_\infty}$ has no non-zero finite submodules provided that p is coprime to the orders of the nonsingular parts of the reduced curves $\tilde{E}_{ns}(\mathbb{F}_{Nv})$ at every bad prime v. This is true for all odd p if E has complex multiplication, by [SeTa]. Moreover when $\check{S}_\infty = (0)$ one can show similarly that $\widehat{S_\infty}$ has no non-zero finite submodules for all such p.

Proof. (of Theorem 2). As indicated above, we restrict to the case where $K = \mathbb{Q}, \delta_K = 1$. The generalisation is straightforward but makes the notation very cumbersome. However one vital caveat if one considers an arbitrary prime $\mathfrak{p}$ of a number field K lying above the rational prime p, is that the definitions (3) (respectively, (4)) must be read *strictly as stated.* Namely, one must exclude (respectively, include) *all places above* p and not just $\mathfrak{p}$ as is sometimes the convention.

For the purposes of the proof of Theorem 1 we only require a proof that (vii) implies (iii); hence for the sake of brevity we only give details relevant to this. The following chains of equivalences:

$$\text{(i)} \Leftrightarrow \text{(ii)} \Leftrightarrow \text{(iii)} \Leftrightarrow \text{(iv)} \Leftrightarrow \text{(v)} \Leftrightarrow \text{(vi)}$$

and

$$\text{(vii)} \Leftrightarrow \text{(viii)} \Leftrightarrow \text{(ix)}(\Leftrightarrow \text{(x)})$$

may be deduced from a careful application of the duality theorems of Cassels, Poitou and Tate [Ca], [Mi, I Sect. 6] to the definitions of these objects. One also needs Propositions 3 and 4 of [Gr3] and [P-R3, Lemma 0.2.4].

So we need only show that (say) (vii) implies (v). Since it will cost us no more effort, we prove it in such a way that the implication (i) $\Rightarrow$ (ix) also becomes apparent. The simplifying observation is to note that each of these requires that we show that under certain hypotheses, if a module M which is the direct limit of finite modules $M_{m,n}$ has Λ_c-corank d, then the module $\check{M}$ obtained from the inverse limits under the dual maps has rank $\leqslant d$. Obviously this does not hold in general, but we can draw together enough information in our situation to formulate the following proposition. Define a family of modules $\mathcal{B}_n^{p^m}$ by the exactness of the sequence

$$0 \to \mathcal{B}_n^{p^m} \to H^1(G_{n,\Sigma}, E_{p^m}) \to \prod_{v|\Sigma'} H^1(\mathbb{Q}_{n,v}^c, E_{p^m}),$$

where Σ' is some subset of Σ. We set as usual

$$\mathcal{B}_n = \operatorname{inj}\lim \mathcal{B}_n^{p^m},$$

the inductive limit being taken with respect to the maps on cohomology induced by the inclusion of E_{p^m} in $E_{p^{m+1}}$, and

$$\check{\mathcal{B}}_n = \operatorname{proj}\lim \mathcal{B}_n^{p^m},$$

where the projective limit is taken with respect to the multiplication by p maps. Finally, set

$$\mathcal{B}_\infty = \operatorname{inj}\lim \mathcal{B}_n,$$

inductive limit with respect to restriction maps, and

$$\check{\mathcal{B}}_\infty = \operatorname{proj}\lim \check{\mathcal{B}}_n,$$

the projective limit with respect to the norm (corestriction) maps.

PROPOSITION 3. *With notation as defined above, suppose that $\mathcal{B}_\infty$ has Λ_c-corank d. Then $\check{\mathcal{B}}_\infty$ has Λ_c-rank $\leqslant d$.*

REMARK. Notice that the Selmer group is excluded from consideration by the stipulation on the local conditions.

Proof. From the definition of the modules $\mathcal{B}_n$ it follows easily by [Im] and the fact that the p-cohomological dimension of Γ_c is one, that the kernel and cokernel of the restriction map

$$\mathcal{B}_n \to \mathcal{B}_\infty^{\Gamma_c^{p^n}}$$

are finite; indeed the kernel has order bounded independently of n. The proposition is now an easy consequence of Lemma 1.1(e) of [Wing]. □

So we have shown that (vii) implies (v) (take $\Sigma' = \Sigma$) and that (i) implies (ix) (take Σ' to be empty). This completes our sketch of a proof of Theorem 2. □

We have the following easy corollary of the considerations above. It gives an 'unramified' analogue of the Cassels–Poitou–Tate exact sequence.

PROPOSITION 5. *Let F be any extension of $\mathbb{Q}$ contained in $\mathbb{Q}_\Sigma$ and let p be any prime. Then the following sequence is exact.*

$$\begin{array}{ccccccc} 0 \to & S'_{E|F} & \to & H^1(G_{F,\Sigma}, E_{p^\infty}) & \xrightarrow{\phi'} & \prod_{v|\Sigma\setminus\{p\}} H^1(F_v, E)(p) & \to \cdots \\ & \cdots & \to & \widehat{\check{R}_{E|F}} & \to & H^2(G_{F,\Sigma}, E_{p^\infty}) & \to 0. \end{array}$$

Proof. We merely sketch the proof. Comparing the definition of $\check{R}_{E|F}$ with the usual Cassels–Poitou–Tate exact sequence over F it is enough to show that

$$\ker \hat{\phi}' = \check{R}_{E|F}/H^2(G_{F,\Sigma}, E_{p^\infty})^\wedge. \tag{5}$$

Define a module $\mathcal{G}$ by the exactness of

$$0 \to \ker \hat{\phi}' \to \check{S}_{E|F}/H^2(G_{F,\Sigma}, E_{p^\infty})^\wedge \to \mathcal{G} \to 0.$$

Some diagram chasing shows that

$$\mathcal{G} \hookrightarrow \prod_{\mathfrak{p}|p} E(F_\mathfrak{p})^{*p},$$

so that certainly the natural map in (5) is surjective. But it is also injective as it is defined as the restriction to $\ker \hat{\phi}'$ of the identity map on $\check{S}_{E|F}/H^2(G_{F,\Sigma}, E_{p^\infty})^\wedge$. □

3. Rubin's supersingular 'main conjecture'

We are reduced by Theorem 2 to showing that $\widehat{R_\infty}$ is Λ_c-torsion. We first explain the connection between the Selmer groups of elliptic curves and the Iwasawa theory of imaginary quadratic fields. Rubin's beautiful analogue of the Coates–Wiles main conjecture for ordinary primes will then enable us to translate the original problem into a problem about elliptic units. In addition to the notation of the previous section we need to introduce the usual machinery for Iwasawa theory over the field of complex multiplication, as follows.

3.1. THE PAIR $\{E, p\}$

Henceforth in this paper, E, K, p and $\mathfrak{p}$ will be as in the statement of Theorem 1. So K is an imaginary quadratic field, $\mathcal{O}_K$ its ring of integers, and p an odd rational prime. E is an elliptic curve defined over K with complex multiplication by $\mathcal{O}_K$.

We work always under the constraint that E has *good supersingular reduction* at $\mathfrak{p}$. The completion of K at $\mathfrak{p}$ will be denoted $K_{\mathfrak{p}}$, and $\mathcal{O}_{\mathfrak{p}}$ will denote the ring of integers of $K_{\mathfrak{p}}$.

Fix once and for all an embedding $K \hookrightarrow \mathbb{C}$ and a Weierstrass equation for E over K which is minimal at $\mathfrak{p}$, of the form

$$E\colon y^2 = 4x^3 - g_2 x - g_3,$$

where $g_2, g_3 \in K$. For any such model there is a natural choice of standard invariant differential ω_E, defined by

$$\omega_E = \mathrm{d}x/y.$$

This is a basis for the cotangent space of E at the origin. The pair (E, ω_E) determines uniquely a period lattice $L = L(E, \omega_E)$ defined by

$$L = \left\{ \int_\gamma \omega_E \colon \gamma \in H_1(E(\mathbb{C}), \mathbb{Z}) \right\},$$

which is naturally an $\mathcal{O}_K$-module. Fix Ω_E to be a generator of this module. With this normalization (E, ω_E), we may write explicitly an identification

$$\iota\colon \mathcal{O}_K \xrightarrow{\sim} \mathrm{End}_K(E),$$

which is such that for any $\alpha \in \mathcal{O}_K$, the endomorphism $\iota(\alpha) \in \mathrm{End}_K(E)$ is that which induces multiplication by α on the tangent space to E at the origin. Let $I_K^{\mathfrak{f}}$ be the subgroup of fractional ideals of K relatively prime to the conductor $\mathfrak{f} = \mathfrak{f}_E$ of E over K. Let ϕ_E be the Hecke grossencharacter of K attached to E by the theory of complex multiplication (see [deS, II Sect. 1]). That is, ϕ_E is the unique homomorphism from $I_K^{\mathfrak{f}}$ to $\mathcal{O}_K$ satisfying the following condition. For any ideal $\mathfrak{a}$ of K prime to $\mathfrak{f}$ and any integral ideal $\mathfrak{c}$ of K prime to $\mathfrak{a}$, we have

$$P^{\sigma_{\mathfrak{a}}} = \iota(\phi_E(\mathfrak{a}))(P)$$

for all $P \in E_{\mathfrak{c}}$, where $\sigma_{\mathfrak{a}}$ is the global Artin symbol for the extension $K(E_{\mathfrak{c}}) : K$.

3.2. p-POWER DIVISION POINTS AND THE TOWER OF FIELDS

We follow [Ru2]. Denote by Φ the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$. For each $n \geqslant 0$ we define $K_n = K(E_{\mathfrak{p}^{n+1}})$ and $\Phi_n = \Phi(E_{\mathfrak{p}^{n+1}})$. Note that the extension $\Phi_n : \Phi$ is totally ramified for all $n \geqslant 0$, by Lubin–Tate theory, so that we may write just $\mathfrak{p}$ for the unique prime of K_n above $\mathfrak{p} \in K$, for every n. So the canonical embedding $K \hookrightarrow \Phi$ fixes embeddings $K_n \hookrightarrow \Phi_n$ for every $n \geqslant 0$. Define $K_\infty = \cup_{n\geqslant 0} K_n$ and $\Phi_\infty = \cup_{n\geqslant 0}\Phi_n$, so we have a fixed embedding of K_∞ into Φ_∞. We may identify $\mathrm{Gal}(K_\infty|K)$ with $\mathrm{Gal}(\Phi_\infty|\Phi)$ since $\mathfrak{p}$ is totally ramified. Fix, once and for all, embeddings of K into $\bar{\mathbb{Q}}$ and $\overline{\mathbb{Q}_p}$, and then embeddings of $\bar{\mathbb{Q}}$ and $\overline{\mathbb{Q}_p}$ into $\mathbb{C}$ so that the compositions of embeddings are compatible with our fixed embedding of K into $\mathbb{C}$. Define $F = K(E_{\mathfrak{f}})$. For every $n \geqslant 0$, define $F_n = F \cdot K_n$. Finally, define $F_\infty = \cup_{n\geqslant 0} F_n = F(E_{\mathfrak{f}\mathfrak{p}^\infty})$.

We shall constantly be making use of the structure which E has locally as a Lubin–Tate formal group. So let Δ denote the unique (cyclic) subgroup of $\mathrm{Gal}(K_\infty|K) = \mathrm{Gal}(\Phi_\infty|\Phi)$ of order $N\mathfrak{p} - 1$, where N denotes the absolute norm. Let K_∞^Δ be the maximal subfield of K_∞ fixed by Δ and let Γ^- be the group $\mathrm{Gal}(K_\infty^\Delta|K_\infty^c)$. We identify $\Gamma_c = \mathrm{Gal}(K_\infty^c|K)$, the galois group of the cyclotomic $\mathbb{Z}_p$-extension of K, with the subgroup $\mathrm{Gal}(K_\infty^\Delta|K_\infty^a)$ of $\mathrm{Gal}(K_\infty|K)$. Here K_∞^a is the 'anticyclotomic' $\mathbb{Z}_p$-extension of K; that is, it is the extension corresponding to the -1-eigenspace for the action of $\mathrm{Gal}(K|\mathbb{Q})$ on $\mathrm{Gal}(K_\infty^\Delta|K)$. Using the facts that the whole extension $K_\infty : K$ is abelian and the order of Δ is coprime to p, we may write

$$\mathrm{Gal}(K_\infty|K) \cong \Gamma_c \times \Gamma^- \times \Delta.$$

Let

$$\Lambda_2 = \mathcal{O}_\mathfrak{p}[[\mathrm{Gal}(K_\infty^\Delta|K)]]$$

be the full 2-variable Iwasawa algebra for our extension of p-power division points. Without loss of generality we choose an identification of Λ_2 with $\mathcal{O}_\mathfrak{p}[[S, T]]$ which is such that $\sigma = (S+1)$ topologically generates the galois group of the cyclotomic extension $K_\infty^c : K$, and $\tau = (T + 1)$ that of the extension $K_\infty^\Delta : K_\infty^c$. That is,

$$\langle\sigma\rangle = \Gamma_c, \quad \langle\tau\rangle = \Gamma^-.$$

Finally, for any field F we let $A(F)$ denote the p-primary part of the ideal class group of F, and write

$$A_\infty = \mathrm{proj\,lim}\, A(K_n),$$

where the projective (inverse) limit is taken with respect to the norm maps.

3.3. Translation of the problem to K_∞

Recall that we are trying to show that $\widehat{R_\infty} = \widehat{R_{E|K_\infty^c}}$ is Λ_c-torsion. We need to link the Selmer groups of E to the Iwasawa theory of K. Write

$$\Lambda_2(\mathbb{Z}_p) = \mathbb{Z}_p[[\mathrm{Gal}(\Phi_\infty|\Phi_0)]],$$

so

$$\Lambda_2 = \Lambda_2(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p}.$$

PROPOSITION 6. *Let E/K and $\mathfrak{p}$ be as in the statement of Theorem 1. Then for all such supersingular $\mathfrak{p}$ we have the following isomorphism of Λ_c-modules:*

$$\widehat{R_\infty} \cong (\widehat{R_{E|K_\infty}})_{\Gamma^- \times \Delta}.$$

PROPOSITION 7. *With notation as in Proposition 6,*

$$\widehat{R_{E|K_\infty}} \cong \mathrm{Hom}_{\mathbb{Z}_p}(T_pE, A_\infty),$$

and they are both $\Lambda_2(\mathbb{Z}_p)$-torsion $\Lambda_2(\mathbb{Z}_p)$-modules.

Propositions 6 and 7 may be found in [Bi, Sect. 3] under slightly more restrictive hypotheses; the generalizations are obvious. □

If ϵ is any $\mathcal{O}_\mathfrak{p}^\times$-valued character of Δ and M any $\mathcal{O}_\mathfrak{p}[\Delta]$-module then we denote by M^ϵ the maximal submodule of M on which Δ acts via the character ϵ. If we define the *ϵ-idempotent* $\iota_\epsilon \in \mathcal{O}_\mathfrak{p}[\Delta]$ as usual by:

$$\iota_\epsilon = \frac{1}{\#\Delta}\sum_{\delta\in\Delta}\delta^{-1}\epsilon(\delta),$$

then we have

$$M^\epsilon = \iota_\epsilon(M).$$

Let κ be the $\mathcal{O}_\mathfrak{p}^\times$-valued character giving the action of galois on the Tate module T_pE, and write ω for κ restricted to the subgroup Δ. Alternatively viewed, κ is the natural isomorphism from $\mathrm{Gal}(\Phi_\infty|\Phi)$ to $\mathcal{O}_\mathfrak{p}^\times$. One has a natural identification of κ with what may loosely be termed the 'p-adic completion of ϕ_E': for a beautiful exposition see [G, Sect. 8]. Notice that we are using here the assumption that $\mathfrak{p}$ is a prime of good reduction, so that $\Phi_\infty : \Phi$ is a Lubin–Tate extension. Define

$$e(T) = (\kappa^{-1}(\tau)\cdot(T+1) - 1). \tag{6}$$

PROPOSITION 8. *With notation as above, $\widehat{R_\infty}$ is Λ_c-torsion if and only if $e(T)$ does not divide the characteristic power series $f(S,T)$ of the Λ_2-module*

$$(A_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p})^\omega.$$

Proof. Let $g(S,T)$ denote a choice of characteristic power series for

$$\mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(T_pE, (A_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p})^\omega)$$

over Λ_2, so that by linear algebra

$$f(S,T) = g(\kappa^{-1}(\sigma)\cdot(S+1) - 1, \kappa^{-1}(\tau)\cdot(T+1) - 1).$$

It is clear that $e(T)$ divides $f(S,T)$ if and only if T divides $g(S,T)$. Let M be any $\mathbb{Z}_p[\Delta]$-module. Then by standard linear algebra we have that as $\mathbb{Z}_p$-modules,

$$\mathrm{Hom}_{\mathbb{Z}_p}(T_pE, M)^{\Delta} \cong \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(T_pE, (M \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p})^{\omega}).$$

Such an isomorphism is easily constructed to preserve the Γ_2-module structure. The question of whether T annihilates anything in these modules is independent of whether we are working over $\mathbb{Z}_p$ or over $\mathcal{O}_\mathfrak{p}$, so we need only show that T divides a characteristic power series for the left-hand module if and only if $\widehat{R_\infty}$ is Λ_c-torsion. But this is exactly proposition 6 combined with proposition 7, using our identification $\langle T+1\rangle = \langle\tau\rangle = \Gamma^-$. □

It is the statement in proposition 8 which we shall now prove. We use Rubin's theorem to convert it to a statement on elliptic units, as follows.

3.4. Local, global and elliptic units

For every $n \geqslant 0$, let U_n denote the group of *principal local units* of Φ_n. These are the units which are congruent to 1 modulo to maximal ideal of the ring of integers of Φ_n. Define U_∞ to be the projective limit with respect to the norm maps of the modules $U_n \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p}$. For each n, let $\mathcal{E}_{n,g}$ denote the group of units of the field K_n, and we let $\mathcal{C}_{n,g}$ denote the subgroup of *elliptic units* as defined in [deS, II Sect. 2]. Each of these $\mathbb{Z}[\mathrm{Gal}(K_n|K)]$-modules sits inside the local field Φ_n. Identifying each with its image inside Φ_n, define $\mathcal{E}_{n,l} = \mathcal{E}_{n,g} \cap U_n$ and similarly $\mathcal{C}_{n,l} = \mathcal{C}_{n,g} \cap U_n$. Denote by $\overline{\mathcal{E}_n}$ and $\overline{\mathcal{C}_n}$ the p-adic closures inside U_n of $\mathcal{E}_{n,l}$ and $\mathcal{C}_{n,l}$ respectively. As usual we refer to these as the *global units* and the *elliptic units* respectively, of the fields Φ_n. Since Leopoldt's conjecture is known for these towers of fields we may identify $\overline{\mathcal{E}_n}$ (respectively, $\overline{\mathcal{C}_n}$) with $\mathcal{E}_{n,l} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ (respectively, $\mathcal{C}_{n,l} \otimes_{\mathbb{Z}} \mathbb{Z}_p$). Define

$$\overline{\mathcal{E}_\infty}^{\omega} = \text{proj lim}(\overline{\mathcal{E}_n} \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p})^{\omega}$$

and

$$\overline{\mathcal{C}_\infty}^{\omega} = \text{proj lim}(\overline{\mathcal{C}_n} \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p})^{\omega},$$

which are naturally submodules of U_∞^{ω}, the projective limits always being taken with respect to the norm maps. It is clear from the definitions that $U_\infty^{\omega}, \overline{\mathcal{E}_\infty}^{\omega}$ and $\overline{\mathcal{C}_\infty}^{\omega}$ are naturally Λ_2-modules. If M is any Λ_2-torsion Λ_2-module, we denote by $f_M = f_M(S,T)$ a choice of characteristic power series for M over Λ_2. We are now in a position to state the following special case of Rubin's supersingular 'main conjecture'.

THEOREM 9 (Rubin). *Let E, p, $\overline{\mathcal{E}_\infty}^{\omega}$, $\overline{\mathcal{C}_\infty}^{\omega}$, A_∞^ω be as above. Then $\overline{\mathcal{E}_\infty}^{\omega}$ and $\overline{\mathcal{C}_\infty}^{\omega}$ are both Λ_2-torsion-free Λ_2-modules of Λ_2-rank one. Moreover, up to a unit in Λ_2,*

$$f_{A_\infty^\omega} \quad \textit{equals} \quad f_{\overline{\mathcal{E}_\infty}^{\omega}/\overline{\mathcal{C}_\infty}^{\omega}}.$$

Proof. See [Ru4, 4.1(ii), 7.8]. □

So the proof of Theorem 1 has been reduced to a proof that a characteristic power series for $\overline{\mathcal{E}_\infty}^{\omega}/\overline{\mathcal{C}_\infty}^{\omega}$ cannot be divisible by the factor $e(T)$ defined in (6). Observe that by Theorem 9 once again, both modules $\overline{\mathcal{E}_\infty}^{\omega}$ and $\overline{\mathcal{C}_\infty}^{\omega}$ are Λ_2-torsion-free of rank one and so $\overline{C_\infty}^{\omega}$ must essentially sit inside $\overline{\mathcal{E}_\infty}^{\omega}$ as a 'multiple' by an element of Λ_2. It is this observation, made formal in the next section, which enables us to use logarithmic derivatives and the formal properties of Coleman power series, to deduce the theorem from the properties of the elliptic units.

4. Elliptic units and logarithmic derivatives

4.1. Coleman power series

Following Rubin [Ru2, Sect. 2], let $f_\beta(X)$ be the Coleman power series attached to any unit $\beta = (\beta_n) \in U_\infty$. Let $\hat{\lambda}(X)$ be the formal group logarithm map attached to our model of the curve (see [Ru1, Sect. 3] or [Si, IV Sect. 3]), and let $\hat{\lambda}'(X)$ denote its first derivative with respect to X. Define $\mathfrak{D}$ to be the 'intrinsic logarithmic derivative' operator

$$\mathfrak{D} = \frac{1}{\hat{\lambda}'(X)} \cdot \frac{d}{\mathrm{d}X} \log,$$

where log is the usual formal power series expression. That is,

$$(\mathfrak{D}f)(X) = \frac{1}{\hat{\lambda}'(X)} \cdot \frac{f'(X)}{f(X)}.$$

Let χ be a character of $\mathrm{Gal}(\Phi_\infty \mid \Phi) = \mathrm{Gal}(K_\infty \mid K)$ which takes values in $\overline{\mathbb{Q}_p}^\times$, and suppose it has finite order (so it has conductor dividing p^{n+1} for some $n \geqslant 0$). Fix this value of n for the moment. Define an $\mathcal{O}_\mathfrak{p}$-linear homomorphism

$$\delta_n \colon U_\infty \to \Phi_n$$

by

$$\delta_n(\beta) = \mathfrak{D} f_\beta(X) \,|_{X=u_n},$$

where $u = (u_n)$ is a topological generator (over $\mathcal{O}_\mathfrak{p}$) for the Tate module T_pE. With our fixed value of n, sufficiently large that the conductor of our fixed character χ divides p^{n+1}, we define another $\mathcal{O}_\mathfrak{p}$-linear homomorphism

$$\delta_\chi \colon U_\infty \to \Phi_n$$

via:

$$\delta_\chi(\beta) = \frac{1}{p^{n+1}} \sum_{\gamma \in \mathrm{Gal}(\Phi_n | \Phi)} \chi(\gamma)\delta_n(\beta)^\gamma.$$

The definition is in fact independent of the choice of n, provided of course that it is sufficiently large [Ru2, Sect. 2]. We need one important formal property of these maps.

LEMMA 10. *If* χ *is a finite character of* $\mathrm{Gal}(\Phi_\infty \mid \Phi_0), \beta \in U_\infty$ *and if* $g(S,T) \in \Lambda_2$ *then*

$$\delta_\chi(g \cdot \beta) = g(\kappa\chi^{-1}(\sigma) - 1, \kappa\chi^{-1}(\tau) - 1) \cdot \delta_\chi(\beta).$$

Proof. See [Ru2, Sect. 2]. □

Notice that on any units whose projection to the ω-eigenspace is zero, the maps δ_n vanish.

4.2. Hecke L-functions

Let M be any abelian extension of K, and suppose that the least common multiple of the conductors $\mathfrak{f}$ of ϕ_E and of the extension $M \mid K$ is the ideal $\mathfrak{m}$ of K. Recall that we define the *partial Hecke L-functions* for the extension $M \mid K$ by

$$L_\mathfrak{m}(\overline{\phi_E}, s; [\mathfrak{a}, M \mid K]) = \sum_{\mathfrak{d}} \overline{\phi_E}(\mathfrak{d})/N\mathfrak{d}^s,$$

where the sum is over all integral ideals $\mathfrak{d}$ of K prime to $\mathfrak{m}$ such that the global Artin symbol $[\mathfrak{d}, M \mid K]$ is equal to $[\mathfrak{a}, M \mid K]$.

Let χ be a complex character of $\mathrm{Gal}(K_\infty \mid K)$ of finite order, and fix an integer $n \geqslant 0$ large enough so that the conductor of χ divides p^{n+1}, as before. We define the L-function twisted by χ as follows (see [Ru1, Sect. 2]):

$$L(\overline{\phi_E}\chi, s) = \left(\sum_{\gamma \in \mathrm{Gal}(\Phi_n | \Phi)} \chi(\gamma) \cdot L_{\mathfrak{f}p}(\overline{\phi_E}, s; \gamma) \right) \times \prod_{\mathfrak{q} \in Q} \left(1 - \frac{\overline{\phi_E}\chi(\mathfrak{q})}{N\mathfrak{q}^s}\right)^{-1},$$

where Q is the finite set of primes which divide $\mathfrak{f}p$ but not the conductor of $\overline{\phi_E}\chi$ (so we just add in the Euler factor at p if χ is the trivial character). Note that we have written $\chi(\mathfrak{q})$ for $\chi([\mathfrak{q}, K_n \mid K])$.

The next result is the key to the entire theory.

THEOREM 11 (Coates–Wiles). *With notation as above, there exists a* single elliptic unit $\vartheta \in \overline{\mathcal{C}_\infty}^{\omega}$ *such that for any character* χ *of* $\mathrm{Gal}(\Phi_\infty \mid \Phi)$ *of finite order,*

$$\delta_\chi(\vartheta) = \Omega_E^{-1}\left(1 - \frac{\overline{\phi_E((p))}}{p^2}\right) \cdot L(\overline{\phi_E}\chi, 1). \tag{7}$$

This result is stated as Theorem 3.2 of [Ru2]. The proof can be pieced together using results from [CW] or [deS]. See also [Ru1]. □

5. Proof of the main theorem

Summarising the algebraic results above, we have reduced the proof of Theorem 1 to the following proposition, whose proof will occupy the remainder of the paper.

PROPOSITION 12. $e(T)$ *is coprime to* $f(S,T)$.

REMARK. The proposition just stated is actually true whenever σ, τ are *any* choice of generators of Γ_2 except possibly when $\langle\sigma\rangle$ is the anticyclotomic extension. This follows from a generalisation by Greenberg of Rohrlich's theorem [Gr2], and has some very strong consequences for the class field theory of K_∞. For a fuller discussion see [McY].

Using Theorem 9 we may identify a characteristic power series $f(S,T)$ in Λ_2 of $(A_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p})^\omega$, with a characteristic power series for

$$\overline{\mathcal{E}_\infty}^{\omega}/\overline{\mathcal{C}_\infty}^{\omega}.$$

A priori the fact that $\overline{\mathcal{E}_\infty}^{\omega}$ is torsion-free of rank one over Λ_2 (theorem 9) is enough to show that theorem 1 is true. Indeed, since the following modules are pseudo-isomorphic (see Lemma 14 below – one needs the fact that any torsion-free rank one Λ_2-module is pseudo-isomorphic to a free module)

$$\overline{\mathcal{E}_\infty}^{\omega}/f\overline{\mathcal{E}_\infty}^{\omega} \sim \Lambda_2/f\Lambda_2 \sim \overline{\mathcal{E}_\infty}^{\omega}/\overline{\mathcal{C}_\infty}^{\omega}$$

we have the short exact sequence (the injectivity follows from the fact that $f\overline{\mathcal{E}_\infty}^{\omega}$ has no non-zero pseudo-null submodules)

$$0 \to f\overline{\mathcal{E}_\infty}^{\omega} \to \overline{\mathcal{C}_\infty}^{\omega} \to \mathcal{P} \to 0,$$

where $\mathcal{P}$ is pseudo-null. Now $f(S,T)$ gives us a natural expression for the elliptic units in $\overline{\mathcal{C}_\infty}^{\omega}$ in terms of the global units $\overline{\mathcal{E}_\infty}^{\omega}$, at least up to the module $\mathcal{P}$. It is easy to show by purely formal algebraic arguments that $\mathcal{P}$ is 'small enough' to allow us essentially to take our $\vartheta \in \overline{\mathcal{C}_\infty}^{\omega}$ to be of the form $f \cdot \eta$ for some $\eta \in \overline{\mathcal{E}_\infty}^{\omega}$. That is, we can translate ϑ by a small distance inside $\overline{\mathcal{C}_\infty}^{\omega}$ without losing arithmetic information. However, for precision and because of future applications of this result (see [McY]), we show that in fact $\mathcal{P}$ is zero.

PROPOSITION 13. *With notation as above,*

$$U_\infty^\omega \cong \Lambda_2^2$$

and the Λ_2-modules

$$\overline{\mathcal{C}_\infty}^{\omega} \quad \text{and} \quad \overline{\mathcal{E}_\infty}^{\omega}$$

are free of rank one.

Proof. The statement about U_∞^ω follows from the main theorem of [Wint]. For the elliptic units we use [Ru4, 7.7(i)], from which the assertion follows easily for the eigenspace in which we are interested. For the global units we shall need a general lemma on Iwasawa algebras.

LEMMA 14. *Let Γ be a Galois group isomorphic to $\mathbb{Z}_p^{d-1}$ for some $d \geqslant 2$. Let $\Lambda = \mathcal{O}[[\Gamma]] \cong \mathcal{O}[[T_1, \dots, T_{d-1}]]$ be the Iwasawa algebra over $\mathcal{O}$, where $\mathcal{O}$ is the ring of integers in some finite extension of $\mathbb{Z}_p$. Suppose that the following sequence of Λ-modules is exact:*

$$0 \to L \to \Lambda^s \to \mathcal{K} \to 0, \tag{8}$$

where we stipulate that if $d \geqslant 3$ then L must have Λ-rank 1. Then the following statements are equivalent.

(i) *L is free (as a Λ-module);*
(ii) *$\mathcal{K}$ has projective dimension $pd_\Lambda(\mathcal{K}) \leqslant 1$;*
(iii) *$\mathcal{K}$ has no non-zero pseudo-null submodules.*

Proof. We omit the full proof as it would take us too far afield. That (i) implies (ii) is obvious. That (ii) implies (iii) follows from a result of Serre [Sel, IV-16, Proposition 7] which says that any ideal $\mathfrak{q}$ associated to the Λ-module M satisfies

$$\mathrm{depth}_\Lambda(M) \leqslant \dim(\Lambda/\mathfrak{q}).$$

The proof that (iii) implies (i) when $d = 2$ is easy: one uses the four-term exact sequence obtained from taking Γ-cohomology of (8) and the fact that L is free if and only if its Γ-coinvariants have no finite submodule. Nakayama's lemma then completes the proof. In general one may prove it by a direct method analogous to this; however it follows from a far more general statement on reflexive modules over Krull domains. See Section 4.1 example (1), Section 4.2 example (2) and proposition 7 of [Bo, VII]. □

We now apply the lemma to the global units. Class field theory gives us an exact sequence of Λ_2-modules (see for example [Ru4, Sect. 4]):

$$0 \to \overline{\mathcal{E}_\infty}^{\omega} \to U_\infty^{\omega} \to (X_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}})^{\omega} \to (A_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}})^{\omega} \to 0,$$

where X_∞ is the galois group of the maximal pro-p-extension of K_∞ unramified outside the prime above p. So in particular,

$$U_\infty^{\omega}/\overline{\mathcal{E}_\infty}^{\omega} \hookrightarrow (X_\infty \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}})^{\omega}$$

and a theorem of Greenberg [Gr1, Proposition 5] says that X_∞ has no non-zero pseudo-null submodules. So we are in the situation of the lemma, since the global units have rank one by Theorem 9. So we conclude that the global units are free. This completes the proof of Proposition 13. □

REMARK. We point out that the conclusions of Proposition 13 are true for any eigenspaces $(\ )^{\nu}$, with slight modifications only in the cases where ν is the trivial character or else the character giving the action of Δ on the pth roots of unity. See [Ru4, Sections 5,7].

We now complete the proof of Proposition 12. Let $\chi\colon \Gamma_2 \to \overline{\mathbb{Q}_p}^{\times}$ be a character of $\Gamma_2 \times \Delta$ of finite order which satisfies $\chi(\tau) = 1$. (That is, χ factors through Γ_c). Then since $e(\kappa(\tau) - 1) = 0$, Lemma 10 shows that the hypothesis that $e(T)$ divided $f(S,T)$ would force $\delta_\chi(f \cdot \eta)$ to be zero. Now χ was arbitrary, so we conclude that if $e(T)$ divides $f(S,T)$ then

$$\delta_\chi(f \cdot \eta) = 0 \text{ for all characters } \chi \text{ factoring through } \Gamma_c. \tag{9}$$

But we have just shown that both $\overline{\mathcal{E}_\infty}^{\omega}$ and $\overline{\mathcal{C}_\infty}^{\omega}$ are free of rank one. Hence

$$\overline{\mathcal{C}_\infty}^{\omega} \cong f(S,T) \cdot \overline{\mathcal{E}_\infty}^{\omega},$$

so by (7), statement (9) implies that

$$L(\overline{\phi_E}\chi, 1) = 0$$

for all χ of cyclotomic type. If we identify as usual the p-adic characters of cyclotomic type with their complex counterparts, this contradicts the following deep theorem of Rohrlich [Ro], generalised by Greenberg [Gr2].

THEOREM 15 (Rohrlich/Greenberg). *With notation as above, for all but finitely many χ the L-function $L(\overline{\phi_E}\chi, s)$ is non-zero at $s = 1$.* □

So the hypothesis that $e(T)$ divides the characteristic power series $f(S,T)$ must be false, and the proof of Proposition 12 (and so of Theorem 1) is complete. □

Acknowledgements

It is a pleasure to thank John Coates for his great insight and encouragement during this work, and for his comments on an earlier version of this paper. I would also like to thank Karl Rubin and Ralph Greenberg for their immensely helpful suggestions.

References

[Bi] Billot, P.: Quelques aspects de la descente sur une courbe elliptique dans le cas de réduction supersingulière, *Compos. Math.* 58 (1986), 341–369.

[Bo] Bourbaki, N.: Commutative Algebra. Hermann, Paris 1972.

[Ca] Cassels, J. W. S.: Arithmetic on curves of genus 1, IV, *J. Reine und Angew. Math.*, 207 (1962), 234–246.

[CGr] Coates, J. and Greenberg, R.: Kummer theory for abelian varieties over local fields, *Inv. Math. 124* (1996), 129–174.

[CMc] Coates, J. and McConnell, G.: On the Iwasawa theory of modular elliptic curves of analytic rank $\leqslant 1$, to appear in Jnl. Lon. Math. Soc.

[CW] Coates, J. and Wiles, A.: On the Conjecture of Birch and Swinnerton-Dyer, *Inv. Math.* 39 223–251 (1977).

[deS] de Shalit, E.: Iwasawa theory for elliptic curves with complex multiplication, *Perspectives in Mathematics 3*, Academic Press, Boston, 1987.

[Grl] Greenberg, R.: On the structure of certain Galois groups, *Invent. Math.* 47 (1978), 85–99.

[Gr2] Greenberg, R.: Non-vanishing of certain values of L-functions, in *Analytic Number Theory and Diophantine Problems*, proceedings of a conference at Oklahoma State University (1984), P.I.M. vol. 70, Birkhäuser Boston 1987.

[Gr3] Greenberg, R.: Iwasawa Theory for p-adic Representations, in *Advanced Studies in Pure Math.* 17, Kinokuniya & Academic Press (1989), 97–137.

[G] Gross, B.: Arithmetic on elliptic curves with complex multiplication, *Lect. Notes Math. 776*, Springer New York (1980).

[Im] Imai, H.: A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_l$-extensions, Proc. Jap. Acad. 51 (1975), 12–16.

[Ko] Kolyvagin, V.: Euler Systems, in *The Grothendieck Festschrift, Volume II*, P.I.M. 87, Birkhäuser Boston 1990.

[Mat] Matsumura, H.: Commutative Ring Theory, C.U.P. Cambridge 1989.

[Mc1] McConnell, G.: On the Iwasawa theory of elliptic curves over cyclotomic fields, Ph.D. thesis, University of Cambridge 1993.

[Mc2] McConnell, G.: On a conjecture of Mazur for modular elliptic curves of analytic rank one, to appear.

[McY] McConnell, G. and Yager, R.: Arithmetic of CM elliptic curves at supersingular primes, in preparation.

[Mi] Milne, J. S.: Arithmetic Duality Theorems, Academic Press Orlando (1986).

[P-R1] Perrin-Riou, B.: Arithmétique des courbes elliptiques et théorie d'Iwasawa, thesis, Soc. Math. de France, Mémoire 17 (1984).

[P-R2] Perrin-Riou, B.: Théorie d'Iwasawa et hauteurs p-adiques: cas des variétés abéliennes, Séminaire de théorie des nombres de Paris 90/91.

[P-R3] Perrin-Riou, B.: Théorie d'Iwasawa et hauteurs p-adiques, *Invent. Math.* 109 (1992), 137–185.

[Ro] Rohrlich, D. E.: On L-functions of elliptic curves and cyclotomic towers', *Invent. Math.* 75, 409–423 (1984).

[Ru1] Rubin, K.: Elliptic curves with complex multiplication and the Conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* 64 (1981), 455–470.

[Ru2] Rubin, K.: Local units, elliptic units, Heegner points and elliptic curves, *Invent. Math.* 88 (1987), 405–422.

[Ru3] Rubin, K.: On the main conjecture of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* 93 (1988) 701–713.

[Ru4] Rubin, K. The 'Main Conjectures' of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* 103 (1991), 25–68.

[Sc] Schneider, P.: p-adic height pairings II, *Inv. Math.* 79, 329–374 (1985).

[Se1] Serre, J.-P.: Algèbre Locale – Multiplicités, Springer-Verlag (2nd edition) 1965.

[Se2] Serre, J.-P. Serre, Local Fields, Springer-Verlag, New York 1979.

[SeTa] Serre, J.-P. and Tate, J.: Good Reduction of Abelian Varieties, *Ann. of Math.* 88 (1968), 492–517.

[Si] Silverman, J.H.: The Arithmetic of Elliptic Curves, Springer-Verlag, New York 1988.

[Ta] Tate, J.: Relations between K_2 and Galois Cohomology, *Invent. Math.* 36, 257–274 (1976).

[Wing] Wingberg, K.: Duality Theorems for Abelian Varieties over $\mathbb{Z}_p$-extensions, *Advanced Studies in Pure Math.* 17, 471–492 (1989).

[Wint] Wintenberger, J.-P.: Structure Galoisienne de limites projectives d'unités locales, *Compos. Math.* 42 1 (1981) 89–103.