Werk

Titel: On the main cojecture of Iwasawa theory for imaginary quadratic fields.

Autor: Rubin, Karl

Jahr: 1988

PURL: https://resolver.sub.uni-goettingen.de/purl?356556735_0093|log34

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Invent. math. 93, 701–713 (1988)

Inventiones mathematicae
© Springer-Verlag 1988

On the main conjecture of Iwasawa theory for imaginary quadratic fields

Karl Rubin*

Department of Mathematics, Ohio State University, 231 W. 18th Avenue, Columbus, OH 43210-1174, USA

Introduction

The main conjecture of Iwasawa theory for imaginary quadratic fields has very important consequences for the arithmetic of elliptic curves with complex multiplication. For a discussion of some of these see [2]. In this paper we prove results in the direction of the main conjecture (Theorem 1.1 for the one-variable conjecture and Theorem 2.1 for the two-variable conjecture) which, although much weaker, still have many significant applications.

In §§1 and 2 we state the one- and two-variable main conjectures and prove Theorems 1.1 and 2.1. In formulating the conjectures we follow the approach given in [5], viewing them purely as conjectures about properties of abelian extensions of imaginary quadratic fields, with no mention of elliptic curves. The proofs of both Theorems 1.1 and 2.1 are based on results proved in [18], which (developing ideas of Thaine [22]) give annihilators of ideal class groups of abelian extensions of imaginary quadratic fields in terms of elliptic units.

In §3 we bring in elliptic curves with complex multiplication and briefly describe the (well-known) connections between such a curve and the Iwasawa modules which appear in the main conjecture. Then in §4 we apply the results of §§1 and 2 to these curves. Theorem 4.2 extends some of the results of [19] (relating the Selmer group of an elliptic curve with the value of its L-function at $s=1$) to a larger class of elliptic curves. Theorem 4.4 proves, for certain CM curves, a conjecture of Mazur on the behavior of the Selmer group over the cyclotomic $\mathbf{Z}_p$-extension. Theorem 4.5 answers a question raised by Greenberg [9] and gives additional evidence for the 2-variable main conjecture.

We begin with two definitions:

§0.1 Elliptic units

Fix an imaginary quadratic field K, and for any ideal $\mathfrak{f}$ of K let $C_\mathfrak{f}$ denote the group of primitive Robert units of conductor $\mathfrak{f}$, for example as defined

* Partially supported by NSF grant DMS-8501937 and by a Sloan fellowship

in Chap. II, §2.7 of [5]. Then $C_{\mathfrak{f}}$ is a subgroup of the group of global units of $K(\mathfrak{f})$, the ray class field of K of conductor $\mathfrak{f}$. If F is an abelian extension of F of conductor $\mathfrak{a}$, we will define the group of elliptic units of F to be

$$C_F = \prod_{\mathfrak{f}|\mathfrak{a}} \mathbf{N}_{FK(\mathfrak{f})/F} C_{\mathfrak{f}}.$$

§0.2 Characteristic ideals

Suppose D is a complete discrete valuation ring with finite residue field and $\Gamma \cong \mathbf{Z}_p^d$ (in this paper we will only be concerned with $d=1$ or 2). Write $\Lambda = \Lambda_{D,\Gamma}$ for the Iwasawa algebra

$$\Lambda = D[\![\Gamma]\!] = \varprojlim D[\Gamma/p^n\Gamma].$$

A finitely generated Λ-module Y is called pseudo-null if its annihilator in Λ has height greater than one; if $\Gamma \cong \mathbf{Z}_p$ then the pseudo-null Λ-modules are exactly the finite modules. Two Λ-modules are said to be pseudo-isomorphic if there is a map between them with pseudo-null kernel and cokernel. Any finitely generated torsion Λ-module Y is pseudo-isomorphic to a module of the form $\bigoplus \Lambda/f_i\Lambda$ for certain $f_i \in \Lambda$, and the characteristic ideal $(\prod f_i)\Lambda$ is a well-defined invariant of Y which we will denote by $\mathrm{char}(Y)$. This invariant satisfies

$$\mathrm{char}(Y)\ Y \text{ is pseudo-null;} \tag{1}$$

$$\text{if } Y' \subset Y, \quad \mathrm{char}(Y/Y')\,\mathrm{char}(Y') = \mathrm{char}(Y). \tag{2}$$

§1. The one-variable conjecture

Fix an imaginary quadratic field K. Let p be an odd rational prime which splits into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}^*$ of K, and let K_∞ denote the unique $\mathbf{Z}_p$-extension of K which is ramified only at $\mathfrak{p}$. Let F_0 be an abelian extension of K, containing the Hilbert class field of K, such that $[F_0 : K]$ is prime to p. These conditions guarantee that $F_0 \cap K_\infty = K$ and that $\mathfrak{p}$ is totally (wildly) ramified in K_∞/K. Set $F_\infty = F_0 K_\infty$, and define $\Delta = \mathrm{Gal}(F_\infty/K_\infty) \cong \mathrm{Gal}(F_0/K)$, $\Gamma = \mathrm{Gal}(F_\infty/F_0) \cong \mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p$, and $G = \mathrm{Gal}(F_\infty/K) = \Delta \times \Gamma$.

We now define various algebraic objects with which the one-variable main conjecture is concerned. For every n write F_n for the extension of F_0 of degree p^n in F_∞, A_n for the p-part of the ideal class group of F_n, E_n for the group of global units of F_n, and C_n for the group of elliptic units of F_n. Write U_n for the group of local units of $F_n \otimes K_{\mathfrak{p}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$, and let $\bar{E}_n$ and $\bar{C}_n$ denote the closures of $E_n \cap U_n$ and $C_n \cap U_n$, respectively, in U_n. Define the inverse limits $A_\infty = \varprojlim A_n$, $E_\infty = \varprojlim \bar{E}_n$, C_∞

$= \varprojlim \bar{C}_n$, and $U_\infty = \varprojlim U_n$, all inverse limits with respect to the norm maps, and define the Iwasawa algebra $\Lambda = \mathbf{Z}_p[\![G]\!] = \varprojlim \mathbf{Z}_p[\mathrm{Gal}(F_n/K)]$. Let M_∞ be the maximal abelian p-extension of F_∞ which is unramified outside of the primes above $\mathfrak{p}$, and write $X_\infty = \mathrm{Gal}(M_\infty/F_\infty)$. Then A_∞, E_∞, C_∞, U_∞, and X_∞ are all finitely generated Λ-modules [11].

Let D denote the extension of $\mathbf{Z}_p$ generated by the values of all characters of Δ into $\bar{\mathbf{Q}}_p^\times$. For any $\mathbf{Z}_p[\Delta]$-module Y and any such character χ of Δ, Y^χ will denote the maximal quotient of $Y \otimes_{\mathbf{Z}_p} D$ on which Δ acts via χ. In particular if Y is a Λ-module then Y^χ is a module over $\Lambda^\chi \cong D[\![\Gamma]\!]$. For every χ, X_∞^χ and $U_\infty^\chi / C_\infty^\chi$ are torsion Λ^χ-modules ([5], §III.1). The following is a version of the main conjecture which avoids mentioning $\mathfrak{p}$-adic L-functions (see §3).

Main conjecture (1-variable). *For any character χ of Δ,*

$$\mathrm{char}(X_\infty^\chi) = \mathrm{char}(U_\infty^\chi / C_\infty^\chi).$$

Theorem 1.1. *For any character χ of Δ, $\mathrm{char}(U_\infty^\chi / C_\infty^\chi)$ annihilates X_∞^χ.*

Theorem 1.1 will follow from Theorem 1.4 below, which is proved using ideas and methods of Thaine [22] as developed in [18]. If χ is nontrivial on the decomposition group of $\mathfrak{p}$ in Δ (which is the case of greatest interest for the applications given later in §4), then Theorem 1.4 follows immediately from Corollary 4.3 and Proposition 4.4 of [18]. The general case will require a little more work.

Fix any topological generator γ of Γ, and for any integers $m \geqq n \geqq 0$ let $\Gamma_{m,n} = \mathrm{Gal}(F_m/F_n) \cong \mathbf{Z}/p^{m-n}\mathbf{Z}$. Write $\hat{H}^0$ and $\hat{H}^{-1}$ for the Tate cohomology groups.

Lemma 1.2. *There is an integer k such that for all $m \geqq n \geqq 0$,*

$$\#[(\gamma - 1)\,\hat{H}^0(\Gamma_{m,n}, E_m)] \leqq p^k \quad \text{and} \quad \#[(\gamma - 1)\,\hat{H}^{-1}(\Gamma_{m,n}, E_m)] \leqq p^k.$$

Proof. For all $m \geqq 0$ let E'_m denote the group of $\mathfrak{p}$-units of F_m, those elements which are units at all primes not dividing $\mathfrak{p}$. Then E_m and E'_m are related by the exact sequence

$$0 \to E_m \to E'_m \to R_m \to 0 \tag{3}$$

where R_m is a submodule of the free $\mathbf{Z}$-module generated by the primes of F_m above $\mathfrak{p}$. Since all primes above $\mathfrak{p}$ are totally ramified in F_∞/F_0, Γ acts trivially on R_m for all m.

By Corollary, §5.4 of [11], there is an integer r such that $\#(\hat{H}^{-1}(\Gamma_{m,n}, E'_m)) \leqq p^r$ for all $m \geqq n \geqq 0$. From (3) we obtain

$$\hat{H}^0(\Gamma_{m,n}, R_m) \to \hat{H}^{-1}(\Gamma_{m,n}, E_m) \to \hat{H}^{-1}(\Gamma_{m,n}, E'_m)$$

and since $\gamma - 1$ kills $\hat{H}^0(\Gamma_{m,n}, R_m)$ we conclude that $\#[(\gamma - 1)\,\hat{H}^{-1}(\Gamma_{m,n}, E_m)] \leqq p^r$ as well.

It is immediate that

$$\hat{H}^0(\Gamma_{m,n}, R_m) = R_m / p^{m-n} R_m \cong (\mathbf{Z}/p^{m-n}\mathbf{Z})^s \quad \text{and} \quad \hat{H}^{-1}(\Gamma_{m,n}, R_m) = 0,$$

where s is the number of primes of F_0 above $\mathfrak{p}$. From (3) and the fact that $E_m \oplus \mathbf{Z}$ contains a subgroup of finite index which is free of rank one over $\mathbf{Z}[\mathrm{Gal}(F_m/K)]$ we conclude that the Herbrand quotient

$$\frac{\#(\hat{H}^0(\Gamma_{m,n}, E'_m))}{\#(\hat{H}^{-1}(\Gamma_{m,n}, E'_m))} = p^{(m-n)(s-1)}.$$

In particular

$$p^{(m-n)(s-1)} \leqq \#(\hat{H}^0(\Gamma_{m,n}, E'_m)) \leqq p^{(m-n)(s-1)+r} \tag{4}$$

for every $m \geqq n \geqq 0$.

Write $\mathbf{N}_{m/n}$ for the norm map from $F_m^\times$ to $F_n^\times$. Then $\mathbf{N}_{n/0}$ induces a surjective map

$$\hat{H}^0(\Gamma_{m,n}, E'_m)/(\gamma-1)\,\hat{H}^0(\Gamma_{m,n}, E'_m) = E'_n/(\mathbf{N}_{m/n} E'_m + (\gamma-1)E'_n) \to \mathbf{N}_{n/0} E'_n/\mathbf{N}_{m/0} E'_m,$$

so we conclude that for all $m \geqq n \geqq 0$,

$$\begin{aligned}\#((\gamma-1)\,\hat{H}^0(\Gamma_{m,n}, E'_m)) &\leqq \frac{\#(\hat{H}^0(\Gamma_{m,n}, E'_m))}{[\mathbf{N}_{n/0} E'_n : \mathbf{N}_{m/0} E'_m]} \\ &= \frac{\#(\hat{H}^0(\Gamma_{m,n}, E'_m))\,\#(\hat{H}^0(\Gamma_{n,0}, E'_n))}{\#(\hat{H}^0(\Gamma_{m,0}, E'_m))} \\ &\leqq p^{2r}\end{aligned}$$

by (4). Now the exact sequence

$$0 \to \hat{H}^0(\Gamma_{m,n}, E_m) \to \hat{H}^0(\Gamma_{m,n}, E'_m)$$

coming from (3) concludes the proof. □

Corollary 1.3. *Let k be the integer of Lemma 1.2. If α is any map from E_∞ to Λ then for every n there is a map β_n from E_n to $\mathbf{Z}_p[\mathrm{Gal}(F_n/K)]$ which makes the following diagram, with the natural vertical maps, commute:*

$$\begin{array}{ccc} E_\infty & \xrightarrow{p^k(\gamma-1)^2\alpha} & \Lambda \\ \downarrow & & \downarrow \\ E_n & \xrightarrow{\beta_n} & \mathbf{Z}_p[\mathrm{Gal}(F_n/K)]. \end{array}$$

Proof. Write $\mathfrak{a}_n$ for the ideal of Λ generated by $\{\sigma-1 : \sigma \in \mathrm{Gal}(F_\infty/F_n)\}$. Then $\Lambda/\mathfrak{a}_n \cong \mathbf{Z}_p[\mathrm{Gal}(F_n/K)]$, so we obtain from α a map

$$\alpha_n : E_\infty/\mathfrak{a}_n E_\infty \to \mathbf{Z}_p[\mathrm{Gal}(F_n/K)].$$

The projection map from E_∞ to $\bar{E}_n$ fits into an exact sequence

$$0 \to \varprojlim_m \hat{H}^{-1}(\Gamma_{m,n}, E_m) \to E_\infty/\mathfrak{a}_n E_\infty \to \bar{E}_n \to \varprojlim_m \hat{H}^0(\Gamma_{m,n}, E_m) \to 0$$

so by Lemma 1.2, $p^k(\gamma-1)^2\alpha_n$ induces (uniquely) a map β_n defined on all of $\bar{E}_n$. □

Theorem 1.4. *There is an integer t such that $p^t \operatorname{char}(E_\infty^\chi/C_\infty^\chi)$ annihilates A_∞^χ.*

Proof. It is shown in the appendix of [19] that elliptic units are special units in abelian extensions of K, in the sense of [18]. (The proof given in [19] makes the assumption that K has class number one, but the proof in the general case is exactly the same.) Thus we can apply the results of [18]. Also, F_∞ contains at most p p-power roots of unity because $\mathfrak{p}^*$ is tamely ramified in F_∞. As mentioned above, if χ is nontrivial on the decomposition group of $\mathfrak{p}$ in Δ then Theorem 1.4 follows immediately from Corollary 4.3 and Proposition 4.4 of [18].

Let χ be any character of Δ. Since E_∞^χ has Λ^χ-rank 1 ([5], §III.1) we can fix a map $\alpha: E_\infty^\chi \to \Lambda^\chi$ with finite cokernel. Then by (1) there is a j such that $p^j \operatorname{char}(E_\infty^\chi/C_\infty^\chi) \subset \alpha(C_\infty^\chi)$. If χ is not the trivial character, Theorem 3.1 of [18] and Corollary 1.3 show that $p^{k+1}(\gamma-1)^2\,\alpha(C_\infty^\chi)$ annihilates A_n^χ for every n. If χ is the trivial character, then Theorem 1.3 and Lemma 1.6 of [18] and Corollary 1.3 show that $p^{k+1}(\gamma-1)^3\,\alpha(C_\infty^\chi)$ annihilates A_n^χ for every n. Therefore for any χ, $p^{j+k+1}(\gamma-1)^3 \operatorname{char}(E_\infty^\chi/C_\infty^\chi)$ annihilates A_∞^χ.

To complete the proof of the theorem it will suffice to show that the kernel of $(\gamma-1)$ acting on A_∞ is finite. Since A_∞ is finitely generated over Λ this will follow if we show that $A_\infty/(\gamma-1)A_\infty$ is finite, and we can identify $A_\infty/(\gamma-1)A_\infty \cong \operatorname{Gal}(L/F_\infty)$ where L is the maximal abelian extension of F_0 in M_∞ which is everywhere unramified over F_∞ ([11] §3.1). Since Leopoldt's conjecture is true for F_0, F_∞ is the unique $\mathbf{Z}_p$-extension of F_0 which is unramified outside the primes above $\mathfrak{p}$ (see [1] p. 123). Thus $\operatorname{Gal}(L/F_\infty)$, which is finitely generated over $\mathbf{Z}_p$, must be finite and the theorem follows. □

Proof of Theorem 1.1. By (2),

$$\operatorname{char}(U_\infty^\chi/C_\infty^\chi) = \operatorname{char}(U_\infty^\chi/E_\infty^\chi)\operatorname{char}(E_\infty^\chi/C_\infty^\chi).$$

Class field theory gives an exact sequence

$$0 \to U_\infty^\chi/E_\infty^\chi \to X_\infty^\chi \to A_\infty^\chi \to 0,$$

so (1) and Theorem 1.4 show that there is an integer h such that $p^h \operatorname{char}(U_\infty^\chi/C_\infty^\chi)$ annihilates X_∞^χ. But by [8] (top of p. 94) and [6] (Théorème 3.4), X_∞ has no p-torsion, so $\operatorname{char}(U_\infty^\chi/C_\infty^\chi)$ annihilates X_∞^χ. □

If ρ is any continuous character of Γ into $\mathbf{C}_p^\times$ (where $\mathbf{C}_p$ is the completion of $\bar{\mathbf{Q}}_p$), ρ extends uniquely to a homomorphism from $\Lambda^\chi \cong D[\![\Gamma]\!]$ to $\mathbf{C}_p$. Theorem 1.1 has the following immediate corollary.

Corollary 1.5. *Let χ be a character of Δ, and fix any generators f_χ of $\mathrm{char}(X_\infty^\chi)$ and g_χ of $\mathrm{char}(U_\infty^\chi/C_\infty^\chi)$.*

(i) *Every irreducible factor of f_χ must divide g_χ.*

(ii) *For every continuous character ρ of Γ, if $\rho(f_\chi)=0$ then $\rho(g_\chi)=0$.* □

§2. The two-variable conjecture

Let K, p, $\mathfrak{p}$, F_0, and Δ be as in §1 (recall F_0 is an abelian extension of K, containing the Hilbert class field of K, such that $[F_0:K]$ is prime to p, and $\Delta=\mathrm{Gal}(F_0/K)$). Let $\mathscr{K}_\infty$ denote the unique $\mathbf{Z}_p^2$-extension of K and set $\mathscr{F}_\infty=F_0\mathscr{K}_\infty$. Then $F_0\cap\mathscr{K}_\infty=K$, and we define $\Gamma_2=\mathrm{Gal}(\mathscr{F}_\infty/F_0)\cong\mathrm{Gal}(\mathscr{K}_\infty/K)\cong\mathbf{Z}_p^2$, and $\mathscr{G}=\mathrm{Gal}(\mathscr{F}_\infty/K)=\Delta\times\Gamma_2$.

We now define the two-variable analogues of the various algebraic objects of §1. For every n write $\mathscr{F}_n$ for the extension of F_0 in $\mathscr{F}_\infty$ with $\mathrm{Gal}(\mathscr{F}_n/F_0)\cong(\mathbf{Z}/p^n\mathbf{Z})^2$, $\mathscr{A}_n$ for the p-part of the ideal class group of $\mathscr{F}_n$, $\mathscr{E}_n$ for the group of global units of $\mathscr{F}_n$, and $\mathscr{C}_n$ for the group of elliptic units of $\mathscr{F}_n$. Write $\mathscr{U}_n$ for the group of local units of $\mathscr{F}_n\otimes K_\mathfrak{p}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$, and let $\bar{\mathscr{E}}_n$ and $\bar{\mathscr{C}}_n$ denote the closures of $\mathscr{E}_n\cap\mathscr{U}_n$ and $\mathscr{C}_n\cap\mathscr{U}_n$, respectively, in $\mathscr{U}_n$. Define the inverse limits $\mathscr{A}_\infty=\varprojlim\mathscr{A}_n$, $\mathscr{E}_\infty=\varprojlim\bar{\mathscr{E}}_n$, $\mathscr{C}_\infty=\varprojlim\bar{\mathscr{C}}_n$, and $\mathscr{U}_\infty=\varprojlim\mathscr{U}_n$, and define the Iwasawa algebra $\Lambda_2=\mathbf{Z}_p[\![\mathscr{G}]\!]$. Let $\mathscr{M}_\infty$ be the maximal abelian p-extension of $\mathscr{F}_\infty$ which is unramified outside of the primes above $\mathfrak{p}$, and write $\mathscr{X}_\infty=\mathrm{Gal}(\mathscr{M}_\infty/\mathscr{F}_\infty)$. Then $\mathscr{A}_\infty$, $\mathscr{E}_\infty$, $\mathscr{C}_\infty$, $\mathscr{U}_\infty$, and $\mathscr{X}_\infty$ are all Λ_2-modules.

Recall that D is the extension of $\mathbf{Z}_p$ generated by the values of all characters of Δ into $\bar{\mathbf{Q}}_p^\times$. If Y is a Λ_2-module and χ is such a character of Δ, then Y^χ is a module over $\Lambda_2^\chi\cong D[\![\Gamma_2]\!]$. For any χ, $\mathscr{X}_\infty^\chi$ and $\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi$ are finitely generated torsion Λ_2^χ-modules [14, 24].

Main conjecture (2-variable). *For any character χ of Δ,*

$$\mathrm{char}(\mathscr{X}_\infty^\chi)=\mathrm{char}(\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi).$$

If F_0 contains the group $\boldsymbol{\mu}_p$ of pth roots of unity, let $\omega\colon\Delta\to\mathbf{Z}_p^\times$ be the character giving the action of Δ on $\boldsymbol{\mu}_p$.

Theorem 2.1. *Let χ be a character of Δ, and if F_0 contains $\boldsymbol{\mu}_p$ suppose that there is no $\sigma\in\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ such that $\chi\chi^\sigma=\omega$. Then $\mathrm{char}(\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi)^2$ annihilates $\mathscr{X}_\infty^\chi$.*

Theorem 2.1 will follow from the following result.

Theorem 2.2. *For any character χ satisfying the hypothesis of Theorem 2.1, $\mathrm{char}(\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi)\mathscr{A}_\infty^\chi$ is pseudo-null.*

Proof. Just as with Theorem 1.4, we will use the fact ([19] §12) that elliptic units are special units in abelian extensions of K, and apply the methods of Thaine [22] as developed in [18]. Fix a character χ as in Theorem 2.1. Our condition on χ is equivalent to the assertion that (when $\boldsymbol{\mu}_p\subset F_0$) if ρ is the irreducible $\mathbf{Z}_p$-representation of Δ in which χ occurs, and $\check{\rho}$ is its contragredient,

then $\rho \neq \check{\rho} \otimes \omega$; this is important in applying the results of [18]. Since $\mathcal{U}_\infty^\chi$ has rank 1 over Λ_2^χ (see [23]) we can fix a map $\alpha: \mathcal{U}_\infty^\chi \to \Lambda_2^\chi$ with pseudo-null cokernel. Then there is a height-two ideal $\mathfrak{c}$ such that $\mathfrak{c}\,\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi) \subset \alpha(\mathcal{C}_\infty^\chi)$.

For all n let $\mathfrak{a}_n$ denote the ideal of Λ_2^χ generated by $\{\sigma - 1 : \sigma \in \mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_n)\}$. Let $\Gamma_\mathfrak{p}$ denote the decomposition group of $\mathfrak{p}$ in Γ, and write $\mathfrak{b}$ for the ideal of Λ_2^χ generated by $\{\sigma - 1 : \sigma \in \Gamma_\mathfrak{p}\}$. Since $\Gamma_\mathfrak{p}$ has finite index in Γ (see [13], §II.1 Lemme 3), $\mathfrak{b}$ is a height-two ideal. Suppose n is large enough so that $\mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F}_n) \subset \Gamma_\mathfrak{p}$. By [23] (Théorème, p. 91 and Proposition, p. 92), the kernel and cokernel of the natural map

$$\mathcal{U}_\infty/\mathfrak{a}_n \mathcal{U}_\infty \to \mathcal{U}_n$$

are annihilated by $\mathfrak{b}$. Therefore for any $r, s \in \mathfrak{b}$, $rs\alpha$ induces a map from $\mathcal{U}_n^\chi$ to $\Lambda_2^\chi/\mathfrak{a}_n \Lambda_2^\chi \cong \mathbf{Z}_p[\mathrm{Gal}(\mathcal{F}_n/K)]^\chi$. If χ is nontrivial then Theorem 3.1 of [18] shows that $rs\alpha(\mathcal{C}_\infty^\chi)$ annihilates $\mathcal{A}_n^\chi$. If χ is the trivial character then Theorem 1.3 and Lemmas 1.6, 1.8, and 1.9 of [18] show that $\mathfrak{b} rs\alpha(\mathcal{C}_\infty^\chi)$ annihilates $\mathcal{A}_n^\chi$. In either case, since this holds for all large n and all $r, s \in \mathfrak{b}$ we conclude that $\mathfrak{c}\mathfrak{b}^3\,\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)$ annihilates $\mathcal{A}_\infty^\chi$, and the theorem follows. □

Proof of Theorem 2.1. Class field theory gives an exact sequence

$$0 \to \mathcal{U}_\infty^\chi/\mathcal{E}_\infty^\chi \to \mathcal{X}_\infty^\chi \to \mathcal{A}_\infty^\chi \to 0.$$

By (1) and Theorem 2.2 we conclude that $\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)^2 \mathcal{X}_\infty^\chi$ is pseudo-null. But by [13] (§II.2 Théorème 23) and [8], $\mathcal{X}_\infty$ has no nontrivial pseudo-null submodule, so $\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)^2 \mathcal{X}_\infty^\chi = 0$. □

Corollary 2.3. *Fix any character χ of Δ satisfying the hypothesis of Theorem 2.1, and fix any generators f_χ of $\mathrm{char}(\mathcal{X}_\infty^\chi)$ and g_χ of $\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)$.*

(i) *Every irreducible factor of f_χ must divide g_χ.*

(ii) *For every continuous character ρ of Γ_2, if $\rho(f_\chi) = 0$ then $\rho(g_\chi) = 0$.* □

Remarks. 1. The proof of Theorem 2.1 actually shows that for characters χ as in the theorem, $\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)\,\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{E}_\infty^\chi)$ annihilates $\mathcal{X}_\infty^\chi$.

2. For those χ not satisfying the hypothesis of Theorem 2.1 one can use the results of [18] to obtain the weaker statement

$$\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)^2\, \iota(\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)) \text{ annihilates } \mathcal{X}_\infty^\chi,$$

where (writing ω_∞ for the character giving the action of $\mathcal{G}$ on all p-power roots of unity) ι denotes the involution of Λ_2 which maps σ to $\omega_\infty(\sigma)\sigma^{-1}$ for every $\sigma \in \mathcal{G}$.

3. The obstacle to improving Theorem 2.1 to say that $\mathrm{char}(\mathcal{U}_\infty^\chi/\mathcal{C}_\infty^\chi)$ annihilates $\mathcal{X}_\infty^\chi$ is the lack of an analogue of Lemma 1.2 for a $\mathbf{Z}_p^2$-extension.

§3. Background on elliptic curves with complex multiplication

Let K be an imaginary quadratic field as before, and F a finite abelian extension of K. For the rest of this paper E will denote an elliptic curve defined over

F with complex multiplication by the ring of integers $\mathcal{O}$ of K, with the additional property that

$$F(E_{\text{torsion}})/K \text{ is abelian.} \tag{5}$$

Note that (5) is automatically satisfied if $F=K$.

§ 3.1 Restriction of scalars

To study E it is convenient to introduce the abelian variety $B=\text{Res}_{F/K}E$, the restriction of scalars of E from F to K. This is an abelian variety of dimension $[F: K]$ defined over K, and over F there is an isomorphism $B\cong \prod_{\sigma\in\text{Gal}(F/K)} E^{\sigma}$.

Proposition 3.1. ([7]) (i) $\text{End}_K(B)\otimes\mathbf{Q}=\prod_{i=1}^{r} T_i$, *where the* T_i *are CM fields and* $\sum_{i=1}^{r}[T_i: K]=\dim(B)=[F: K]$.

(ii) *B is isogenous over F to $E^{[F: K]}$.*

Proof. This is proved in [7] Théorème 4.1 and Lemme 4.2, using the property (5). □

Let $K_{\mathbf{A}}^{\times}$ and $F_{\mathbf{A}}^{\times}$ denote the idele groups of K and F, respectively. Write $T=\prod T_i=\text{End}_K(B)\otimes\mathbf{Q}$ and let $\tilde{\psi}$ and $\tilde{\varphi}$ denote the algebraic Hecke characters

$$\tilde{\psi}: F_{\mathbf{A}}^{\times}\to K^{\times}, \qquad \tilde{\varphi}: K_{\mathbf{A}}^{\times}\to T^{\times}$$

attached to E and B, respectively, by Theorem 10 of [20]. Fix once and for all an embedding of F into $\mathbf{C}$. Define complex Hecke characters of F and K by

$$\psi(\mathbf{a})=\tilde{\psi}(\mathbf{a})\prod_{v|\infty} a_v^{-1} \qquad \text{for } \mathbf{a}=(a_v)\in F_{\mathbf{A}}^{\times},$$

and for any $\iota\in\text{Hom}_K(T, \mathbf{C})$

$$\varphi_\iota(\mathbf{a})=\iota(\tilde{\varphi}(\mathbf{a}))/a_\infty \qquad \text{for } \mathbf{a}=(a_v)\in K_{\mathbf{A}}^{\times}.$$

The L-function of E over F is given by $L(E_{/F}, s)=L(\psi, s)\,L(\bar{\psi}, s)$.

Lemma 3.2. *For any* $\iota\in\text{Hom}_K(T, \mathbf{C})$,

(i) $\psi=\varphi_\iota\circ\mathbf{N}_{F/K}$

(ii) $\{\varphi_\alpha | \alpha\in\text{Hom}_K(T, \mathbf{C})\}=\{\varphi_\iota\,\omega | \omega: \text{Gal}(F/K)\to\mathbf{C}^{\times}\}$

(iii) $L(\bar{\psi}, s)=\prod_{\alpha\in\text{Hom}_K(T, \mathbf{C})} L(\bar{\varphi}_\alpha, s)$.

Proof. Assertions (i) and (ii) are proved in [7] Lemme 4.8, and (iii) follows easily by comparing Euler factors. □

Let p be an odd rational prime and $\mathfrak{p}$ a prime of K above p satisfying

(i) p splits into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}^*$ of K,

(ii) p does not divide $[F: K]$,
(iii) $\mathfrak{p}$ is unramified in F/K, and
(iv) E has good reduction at all primes of F above $\mathfrak{p}$.

(Observe that conditions (ii), (iii) and (iv) eliminate only finitely many primes.) Define $F_0 = F(E_\mathfrak{p})$. The classical theory of complex multiplication shows that F (and therefore F_0 as well) contains the Hilbert class field of K. Also, $\mathrm{Gal}(F_0/F)$ injects into $\mathrm{Aut}(E_\mathfrak{p}) \cong (\mathcal{O}/\mathfrak{p})^\times$ so $[F_0: F]$ is prime to p. Thus we can apply the results of §§1 and 2 with this field F_0. Let Δ, F_∞, Γ, X_∞, U_∞, C_∞, etc. and their 2-variable analogues be as in §§1 and 2, and keep the rest of the notation of those sections as well. Note that $F_\infty = F(E_{\mathfrak{p}^\infty})$.

§3.2 The Selmer group

Let $Ш_F$ and S_F denote, respectively, the Tate-Shafarevich group of E over F and the direct limit of the Selmer groups of E relative to powers of $\mathfrak{p}$ (for the definitions see for example [1] (1), (3) and (10)). These groups fit into an exact sequence

$$0 \to E(F) \otimes (K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}) \to S_F \to Ш_F(\mathfrak{p}) \to 0$$

where $Ш_F(\mathfrak{p})$ denotes the $\mathfrak{p}$-power torsion in $Ш_F$. The connection between these groups and X_∞ is given by the following result.

Theorem 3.3 (Coates). *There is a natural injection*

$$S_F \hookrightarrow \mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathrm{Gal}(F_\infty/F)}.$$

For the proof see [1] Theorems 9 and 12. Similarly we can define the Selmer group S_L of E over any algebraic extension L of F. The following extension of Theorem 3.3 was proved by Perrin-Riou in [13] Chapter II, Proposition 12 and Théorème 18.

Theorem 3.4. *Suppose L_∞ is any $\mathbf{Z}_p$-extension of F inside $\mathcal{F}_\infty$ different from FK_∞. Then there is a natural injection*

$$S_{L_\infty} \hookrightarrow \mathrm{Hom}(\mathcal{X}_\infty, E_{\mathfrak{p}^\infty})^{\mathrm{Gal}(\mathcal{F}_\infty/L_\infty)}.$$

§3.3 $\mathfrak{p}$-adic L-functions

Write $\kappa: \Gamma \to 1 + p\mathbf{Z}_p$ for the character giving the action of Γ on $E_{\mathfrak{p}^\infty}$ (or equivalently on $B_{\mathfrak{p}^\infty}$, since B is isogenous over F to $E^{[F:K]}$ by Proposition 3.1(ii)) and write $\varepsilon: \Delta \to (T \otimes K_\mathfrak{p})^\times$ for the character giving the action of Δ on $B_\mathfrak{p}$. Then the product $\kappa\varepsilon$ is the character giving the action of G on $B_{\mathfrak{p}^\infty}$, so for all primes $\mathfrak{q}$ of K prime to $\mathfrak{p}$ and to the conductor of $\tilde{\varphi}$, $\kappa\varepsilon(\mathfrak{q}) = \tilde{\varphi}(\mathfrak{q})$. For $\iota \in \mathrm{Hom}_K(T, \mathbf{C})$ write $\varepsilon_\iota = \iota \circ \varepsilon$.

Lemma 3.5. *For every $\iota \in \mathrm{Hom}_K(T, \mathbf{C})$, ε_ι satisfies the hypothesis of Theorem 2.1.*

Proof. Suppose that $\mu_p \subset F_0$, or else there is nothing to check, and let ω be the character giving the action of Δ on μ_p. Since $\mathfrak{p}$ is unramified in F/K, the restriction of ω to $\mathrm{Gal}(F_0/F)$ must have order $p-1$. The restriction of ε_ι to $\mathrm{Gal}(F_0/F)$ is $\mathbf{Z}_p^\times$-valued, so for any $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$, the restriction of $\varepsilon_\iota \varepsilon_\iota^\sigma = \varepsilon_\iota^2$ has order at most $(p-1)/2$. In particular $\varepsilon_\iota \varepsilon_\iota^\sigma \neq \omega$. □

Let $\mathcal{I}$ denote the ring of integers of the completion of the maximal unramified extension of $\mathbf{Q}_p$, and $\mathbf{C}_p$ the completion of $\bar{\mathbf{Q}}_p$. If ρ is any continuous character of Γ (resp. Γ_2) into $\mathbf{C}_p^\times$, ρ has a unique extension to a continuous homomorphism from $\mathcal{I}[\![\Gamma]\!]$ (resp. $\mathcal{I}[\![\Gamma_2]\!]$) into $\mathbf{C}_p$. Fix once and for all an embedding of $\mathbf{C}_p$ into $\mathbf{C}$; this will allow us to identify complex and $\mathfrak{p}$-adic valued characters.

Fix a generator $\Omega \in \mathbf{C}^\times$ of the period lattice of a model of E which is minimal at all primes above $\mathfrak{p}$.

Theorem 3.6 (Coates-Wiles, de Shalit). *Let $\chi = \varepsilon_\iota$ for some $\iota \in \mathrm{Hom}_K(T, \mathbf{C})$. Then $\mathrm{char}(U_\infty^\chi / C_\infty^\chi)\mathcal{I}[\![\Gamma]\!]$ has a generator $\mathbf{L}_\chi$ such that for all characters ρ of finite order of Γ,*

$$\kappa\rho(\mathbf{L}_\chi) = \Omega^{-1}\tau(\varphi_\iota, \rho)(1 - \varphi_\iota\rho(\mathfrak{p})/p)L(\bar{\varphi}_\iota\rho^{-1}, 1).$$

Here $\tau(\varphi_\iota, \rho)$ is the "Gauss sum" defined in (30), §II.4 of [5]; *$\tau(\varphi_\iota) = 1$ and $\tau(\varphi_\iota, \rho) \neq 0$ for all ρ.*

Proof. This was proved by Coates and Wiles in [4] in the special case $F = K$, and by de Shalit ([5] §III.1) in general. We are making use of the fact that ε_ι is nontrivial, since $F(E_\mathfrak{p}) \neq F$ (see [5] §II.1). □

For the two-variable situation we will need the following result.

Theorem 3.7 (Yager, de Shalit). *Let $\chi = \varepsilon_\iota$ for some $\iota \in \mathrm{Hom}_K(T, \mathbf{C})$. Then $\mathrm{char}(\mathcal{U}_\infty^\chi / \mathcal{C}_\infty^\chi)\mathcal{I}[\![\Gamma_2]\!]$ has a generator $\mathcal{L}_\chi$ such that for all characters ρ of finite order of Γ_2.*

$$\kappa\rho(\mathcal{L}_\chi) = \Omega^{-1}\tau(\varphi_\iota, \rho)(1 - \varphi_\iota\rho(\mathfrak{p})/p)(1 - \bar{\varphi}_\iota\rho^{-1}(\mathfrak{p}^*)/p)\, L(\bar{\varphi}_\iota\rho^{-1}, 1).$$

Here $\tau(\varphi_\iota, \rho)$ is the "Gauss sum" defined in (30), §II.4 of [5], *which is always nonzero.*

Proof. This was proved by Yager in [24] in the special case $F = K$; for the general case see [5]. □

Theorem 3.8. *For every $\iota \in \mathrm{Hom}_K(T, \mathbf{C})$,*

(i) *$\mathbf{L}_{\varepsilon_\iota}$ annihilates $X_\infty^{\varepsilon_\iota}$,*

(ii) *$\mathcal{L}_{\varepsilon_\iota}^2$ annihilates $\mathcal{X}_\infty^{\varepsilon_\iota}$.*

Proof. Theorems 1.1 and 3.6 for (i); Theorems 2.1 and 3.7 and Lemma 3.5 for (ii). □

§4. Applications

Keep the notation of the previous sections.

Lemma 4.1. *Write t for the endomorphism of $\mathcal{I}[\![\Gamma_2]\!]$ which sends $\sigma \in \Gamma_2$ to $\kappa(\sigma)\sigma^{-1}$.*

(i) *For any $f \in \mathcal{I}[\![\Gamma_2]\!]$ and any character ρ of Γ_2, $\rho(t(f)) = \kappa\rho^{-1}(f)$.*

(ii) *If f annihilates the $\mathscr{I}[\![\Gamma_2]\!]$-module Z, then $t(f)$ annihilates* $\mathrm{Hom}(Z, E_{\mathfrak{p}^\infty})$ *and $\kappa(f)$ annihilates* $\mathrm{Hom}(Z, E_{\mathfrak{p}^\infty})^\Gamma$.

Proof. Easy exercise. □

Theorem 4.2. $(\prod_{v|\mathfrak{p}}(1-\psi(v)/\mathbf{N}v))\, L(\bar{\psi}, 1)/\Omega^{[F:K]}$ *annihilates $S_F \otimes \mathscr{I}$. In particular if $L(\bar{\psi}, 1) \neq 0$ then $E(F)$ and $Ш_F(\mathfrak{p})$ are both finite.*

Remarks 1. The assertion about $E(F)$ was proved by Coates and Wiles [3] when $F=K$ and by Arthaud for the fields F considered here; see [5] or [17].

2. When $F=K$, Theorem A of [19] shows that if $L(\bar{\psi}, 1)\neq 0$ then $Ш_F(\mathfrak{p})$ is finite. However, if $\mathfrak{p}\nmid(1-\psi(\mathfrak{p})/p)$ (the "non-anomalous" case) then Theorem 4.2 shows that $L(\bar{\psi}, 1)/\Omega$ annihilates $Ш_F(\mathfrak{p})$, which is stronger than the result of [19].

3. By Theorem 7.1 of [7], $L(\bar{\psi}, 1)/\Omega^{[F:K]} \in F$.

Proof. Since B is isogenous to $E^{[F:K]}$ over F, ε_ι gives the action of $\mathrm{Gal}(F_0/F)$ on $E_{\mathfrak{p}}$ for any $\iota \in \mathrm{Hom}_K(T, \mathbf{C})$. Therefore

$$\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathrm{Gal}(F_\infty/F)} \otimes D \cong \bigoplus_{\omega \text{ of } \mathrm{Gal}(F/K)} \mathrm{Hom}(X_\infty^{\varepsilon_\iota \omega}, E_{\mathfrak{p}^\infty})^\Gamma$$
$$= \bigoplus_{\alpha \in \mathrm{Hom}_K(T, \mathbf{C})} \mathrm{Hom}(X_\infty^{\varepsilon_\alpha}, E_{\mathfrak{p}^\infty})^\Gamma$$

by Lemma 3.2(ii). By Theorem 3.8(i) and Lemma 4.1(ii), $\kappa(\mathbf{L}_{\varepsilon_\alpha})$ annihilates $\mathrm{Hom}(X_\infty^{\varepsilon_\alpha}, E_{\mathfrak{p}^\infty})^\Gamma$ for every α, so $\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathrm{Gal}(F_\infty/F)}$ is annihilated by the least common multiple of the $\kappa(\mathbf{L}_{\varepsilon_\alpha})$. By Theorem 3.6 and Lemma 3.2,

$$\prod_{\alpha \in \mathrm{Hom}_K(T, \mathbf{C})} \kappa(\mathbf{L}_{\varepsilon_\alpha}) = \Omega^{-[F:K]} \prod_{\alpha \in \mathrm{Hom}_K(T, \mathbf{C})} (1-\varphi_\alpha(\mathfrak{p})/p)\, L(\bar{\varphi}_\alpha, 1)$$
$$= (\prod_{v|\mathfrak{p}}(1-\psi(v)/\mathbf{N}v))\, L(\bar{\psi}, 1)/\Omega^{[F:K]}.$$

Therefore by Theorem 3.3, $(\prod_{v|\mathfrak{p}}(1-\psi(v)/\mathbf{N}v))\, L(\bar{\psi}, 1)/\Omega^{[F:K]}$ annihilates S_F. □

Proposition 4.3. *Let L_∞ be any $\mathbf{Z}_p$-extension of F inside $\mathscr{F}_\infty$. Suppose that for every $\iota \in \mathrm{Hom}_K(T, \mathbf{C})$ there is a character ρ of finite order of $\mathrm{Gal}(L_\infty/F)$ such that $L(\bar{\varphi}_\iota \rho, 1) \neq 0$. Then the Pontrjagin dual of S_{L_∞} is a torsion $\mathbf{Z}_p[\![\mathrm{Gal}(L_\infty/F)]\!]$-module.*

Proof. By [1] § 2, the dual of S_{FK_∞} is a torsion $\mathbf{Z}_p[\![\mathrm{Gal}(FK_\infty/F)]\!]$-module, so we may assume $L_\infty \neq FK_\infty$. As in the proof of Theorem 4.2, using Theorem 3.4 and the fact that $\mathrm{Gal}(F_0/F) \subset \mathrm{Gal}(\mathscr{F}_\infty/L_\infty)$ we have

$$S_{L_\infty} \otimes D \subset \mathrm{Hom}(\mathscr{X}_\infty, E_{\mathfrak{p}^\infty})^{\mathrm{Gal}(\mathscr{F}_\infty/L_\infty)} \otimes D \cong \bigoplus_{\iota \in \mathrm{Hom}_K(T, \mathbf{C})} \mathrm{Hom}(\mathscr{X}_\infty^{\varepsilon_\iota}, E_{\mathfrak{p}^\infty})^{\mathrm{Gal}(\mathscr{F}_\infty/L_\infty)}.$$

By Theorem 3.8(ii), $\mathscr{L}_{\varepsilon_\iota}^2$ annihilates $\mathscr{X}_\infty^{\varepsilon_\iota}$, so by Lemma 4.1(ii), $\prod_{\iota \in \mathrm{Hom}_K(T, \mathbf{C})} t(\mathscr{L}_{\varepsilon_\iota})^2$ annihilates S_{L_∞}. If ρ is a character of $\mathrm{Gal}(L_\infty/F)$ such that $L(\bar{\varphi}_\iota \rho, 1) \neq 0$, then

by Lemma 4.1(i) and the formula of Theorem 3.7, $\rho(t(\mathscr{L}_{\varepsilon_\iota}))\neq 0$. Therefore for every ι the projection of $t(\mathscr{L}_{\varepsilon_\iota})$ into $\mathscr{I}[\![\mathrm{Gal}(L_\infty/F)]\!]$ is nonzero, and the proposition follows. □

We can use this proposition to prove a special case of a conjecture of Mazur ([12] p. 184).

Theorem 4.4. *Let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Then the dual of $S_{F\mathbf{Q}_\infty}$ is a torsion $\mathbf{Z}_p[\![\mathrm{Gal}(F\mathbf{Q}_\infty/F)]\!]$-module.*

Proof. By a theorem of Shimura [21], for any $\iota\in\mathrm{Hom}_k(T, \mathbf{C})$ there is a normalized newform f_ι of weight 2, some level and some character such that $L(f_\iota, s)=L(\bar{\varphi}_\iota, s)$. Therefore by a theorem of Rohrlich ([16], Theorem 1; see also [15]), $L(\bar{\varphi}_\iota\rho, 1)\neq 0$ for all but finitely many characters ρ of finite order of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$. Now the theorem follows from Proposition 4.3. □

Let K_∞^- denote the anticyclotomic $\mathbf{Z}_p$-extension of K, the unique $\mathbf{Z}_p$-extension of K which is Galois over $\mathbf{Q}$ and on which $\mathrm{Gal}(K/\mathbf{Q})$ acts via the nontrivial character. We will call φ_ι anticyclotomic if $\varphi_\iota(\mathfrak{a}^\tau)=\bar{\varphi}_\iota(\mathfrak{a})$ for all ideals $\mathfrak{a}$ of K prime to the conductor of φ_ι, where τ denotes the nontrivial automorphism of K. Combining Proposition 4.3 with a forthcoming result of R. Greenberg [10] allows us to generalize Theorem 4.4 as follows. If L_∞ is any $\mathbf{Z}_p$-extension of F in $\mathscr{F}_\infty$ different from FK_∞^-, or if $L_\infty=FK_\infty^-$ and for all $\iota\in\mathrm{Hom}(T, \mathbf{C})$ either φ_ι is not anticyclotomic or $L(\varphi_\iota, s)$ satisfies a functional equation with constant $+1$, then the dual of S_{L_∞} is a torsion $\mathbf{Z}_p[\![\mathrm{Gal}(L_\infty/F)]\!]$-module. Namely, Greenberg proves that under these hypotheses, for all ι and all but finitely many characters ρ of finite order of $\mathrm{Gal}(L_\infty/F)$, $L(\bar{\varphi}_\iota\rho, 1)\neq 0$.

Now suppose $\iota\in\mathrm{Hom}(T, \mathbf{C})$ is such that φ_ι is anticyclotomic, and write $\chi=\varepsilon_\iota$. Fix a topological generator σ of $\mathrm{Gal}(\mathscr{K}_\infty/K_\infty^-)$, and write $\Theta=\sigma-\kappa(\sigma)\in\Lambda_2^\chi$. Using ideas of R. Greenberg we can prove the following theorem, which gives additional evidence for the 2-variable main conjecture.

Theorem 4.5. *With Θ and χ as above,* $\mathrm{ord}_\Theta(\mathrm{char}(\mathscr{X}_\infty^\chi))=\mathrm{ord}_\Theta(\mathrm{char}(\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi))$.

Proof. In this proof all references to Greenberg's paper [9] apply only if $F=K$ and $p>3$; the general statements are all proved in [5] §IV.3. Class field theory gives a fourterm exact sequence

$$0\to\mathscr{E}_\infty^\chi/\mathscr{C}_\infty^\chi\to\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi\to\mathscr{X}_\infty^\chi\to\mathscr{A}_\infty^\chi\to 0$$

of torsion Λ_2^χ-modules, so to prove the theorem it will suffice to show that $\mathrm{ord}_\Theta(\mathrm{char}(\mathscr{A}_\infty^\chi))=\mathrm{ord}_\Theta(\mathrm{char}(\mathscr{E}_\infty^\chi/\mathscr{C}_\infty^\chi))=0$. Let χ' be the character of Δ given by $\chi'(\mathfrak{a})=\chi(\mathfrak{a}^\tau)$, where τ is the nontrivial automorphism of K. By Propositions 1 and 6 of [9], Θ divides one of $\mathrm{char}(\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi)$ and $\mathrm{char}(\mathscr{U}_\infty^{\chi'}/\mathscr{C}_\infty^{\chi'})$ but not both. By Theorem 2.2 and Lemma 3.5 we conclude that Θ cannot divide both $\mathrm{char}(\mathscr{X}_\infty^\chi)$ and $\mathrm{char}(\mathscr{X}_\infty^{\chi'})$, and then Proposition 2 of [9] shows that $\Theta\nmid\mathrm{char}(\mathscr{E}_\infty^\chi/\mathscr{C}_\infty^\chi)$ and $\Theta\nmid\mathrm{char}(\mathscr{A}_\infty^\chi)$. □

Remark. With Θ and ι as in Theorem 4.5, let $w=\pm 1$ denote the constant in the functional equation satisfied by $L(\varphi_\iota, s)$. By Proposition 6 of [9], Θ divides

char $(\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi)$ if and only if $w=-1$. When $w=-1$ it is possible to show, using Theorem 3.7 and recent results of Perrin-Riou, Gross and Zagier, Waldspurger, and Bertrand (see §1.4 of [14]), that ord_{θ} char $(\mathscr{U}_\infty^\chi/\mathscr{C}_\infty^\chi)=1$.

References

1. Coates, J.: Infinite descent on elliptic curves. In: Arithmetic and Geometry, papers dedicated to I.R. Shafarevich on the occasion of his 60th birthday. Prog. Math. **35**, 107–136. Boston: Birkhäuser (1983)
2. Coates, J., Goldstein, C.: Some remarks on the main conjecture for elliptic curves with complex multiplication. Am. J. Math. **105**, 337–366 (1983)
3. Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **39**, 223–251 (1977)
4. Coates, J., Wiles, A.: On p-adic L-functions and elliptic units. J. Austr. Math. Soc. **26**, 1–25 (1978)
5. de Shalit, E.: The Iwasawa Theory of Elliptic Curves with Complex Multiplication. Perspec. Math. **3**, Orlando: Academic Press (1987)
6. Gillard, R.: Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes. J. Reine Angew. Math. **358**, 76–91 (1986)
7. Goldstein, C., Schappacher, N.: Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe. J. Reine Angew. Math. **327**, 184–218 (1981)
8. Greenberg, R.: On the structure of certain Galois groups. Invent Math. **47**, 85–99 (1978)
9. Greenberg, R.: On the Birch and Swinnerton-Dyer conjecture. Invent. Math. **72**, 241–265 (1983)
10. Greenberg, R.: Elliptic curves and $\mathbf{Z}_p$-extensions (To appear)
11. Iwasawa, K.: On $\mathbf{Z}_l$-extensions of algebraic number fields. Ann. Math. **98**, 246–326 (1973)
12. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. **18**, 183–266 (1972)
13. Perrin-Riou, B.: Arithmétique des courbes elliptiques et théorie d'Iwasawa. Mém. Soc. Math. Fr. **17** (1984)
14. Perrin-Riou, B.: Points de Heegner et dérivées de fonctions Lp-adiques. Invent. Math. **89**, 455–510 (1987)
15. Rohrlich, D.: On L-functions of elliptic curves and cyclotomic towers. Invent. Math. **75**, 409–423 (1984)
16. Rohrlich, D.: L-functions and division towers. Math. Ann. (To appear)
17. Rubin, K.: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **64**, 455–470 (1981)
18. Rubin, K.: Global units and ideal class groups. Invent. Math. **89**, 511–526 (1987)
19. Rubin, K.: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. Invent. Math. **89**, 527–560 (1987)
20. Serre, J-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. **88**, 492–517 (1968)
21. Shimura, G.: On elliptic curves with complex multiplication as factors of the jacobians of modular function fields. Nagoya Math. J. **43**, 199–208 (1971)
22. Thaine, F.: On the ideal class groups of real abelian number fields (To appear)
23. Wintenberger, J-P.: Structure galoisienne de limites projectives d'unités locales. Comp. Math. **42**, 89–103 (1981)
24. Yager, R.: On two variable p-adic L-functions. Ann. Math. **115**, 411–449 (1982)

Oblatum 25-III-1988