COMPOSITIO MATHEMATICA

NICOLE ARTHAUD

On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I

Compositio Mathematica, tome 37, nº 2 (1978), p. 209-232

<http://www.numdam.org/item?id=CM_1978__37_2_209_0>

COMPOSITIO MATHEMATICA, Vol. 37, Fasc. 2, 1978, pag. 209–232
Sijthoff & Noordhoff International Publishers – Alphen aan den Rijn
Printed in the Netherlands

ON BIRCH AND SWINNERTON-DYER'S CONJECTURE FOR ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION. I.

Nicole Arthaud

Introduction

Let K be an imaginary quadratic field, and E an elliptic curve with complex multiplication by the ring of integers of K. Assume that E is defined over a finite extension F of K, and let $L(E/F, s)$ be the Hasse-Weil zeta function of E over F. Deuring has proven that $L(E/F, s)$ can be analytically continued over the whole complex plane, by identifying it with a product of Hecke L-series with Grössencharacters (see [7], Theorem 7.42). The conjecture of Birch and Swinnerton-Dyer asserts that $L(E/F, s)$ has a zero at $s = 1$ of order equal to g_F, the rank of the group $E(F)$ of points of E with coordinates in F. Recently, Coates and Wiles [4] made some progress on a weak form of this conjecture. Namely, they showed that if K has class number 1 and $F = K$, then $g_F \geq 1$ implies that $L(E/F, s)$ does indeed vanish at $s = 1$. The aim of the present paper is to extend Coates and Wiles' proof to the case in which K has class number 1, E is still defined over K, but the base field F is now an arbitrary finite abelian extension of K.

THEOREM 1: *Let K be an imaginary quadratic field with class number 1, and E an elliptic curve defined over K, with complex multiplication by the ring of integers of K. If F is a finite abelian extension of K such that E has a point of infinite order with coordinates in F, then $L(E/F, s)$ vanishes at $s = 1$.*

In a subsequent, but considerably more technical, paper [1] in preparation, we shall prove an analogous result when (i) no restriction is made on the class number of K, (ii) the base field F is again supposed to be an abelian extension of K, and finally (iii) the torsion points of E are assumed to generate over F an abelian extension of K (see Theorem 7.44 of [7] for a necessary and sufficient condition for (iii) to be valid for E). Since the methods of [4] depend crucially on the explicit knowledge of class field theory for abelian extensions of K, there seems to be little hope at present of proving results like Theorem 1 without hypotheses (ii) and (iii) above.

The broad outlines of the proof of Theorem 1 follow fairly closely the arguments in [4]. However, there are some significant and interesting innovations in dealing with an arbitrary finite abelian extension of K as base field. In particular, certain partial Hecke L-functions with Grössencharacters play a natural role in the proof. This is in striking analogy with the theory of cyclotomic $\mathbf{Z}_p$-extensions, where the values of partial L-functions formed with characters of finite order give the coefficients of Stickelberger ideals (see [2]). Also, we have simplified the proof of [4] in several cases (cf. the proof of Theorem 19).

In conclusion, I wish to thank John Coates for his guidance with this work.

1. Notation

To a large extent, we follow the notation of [4]. Thus K will denote an imaginary quadratic field with class number 1, lying inside the complex field $\mathbf{C}$, and $\mathcal{O}$ the ring of integers of K. As in the Introduction, E will be an elliptic curve defined over K, whose ring of endomorphisms is isomorphic to $\mathcal{O}$. We fix a Weierstrass model for E

$$y^2 = 4x^3 - g_2x - g_3, \tag{1}$$

where g_2, g_3 belong to $\mathcal{O}$, and where the discriminant of (1) is divisible only by the primes of K where E has a bad reduction, and (possibly) by the primes of K above 2 and 3. Let $\wp(z)$ be the associated Weierstrass function, L the period lattice of $\wp(z)$, and $\xi(z) = (\wp(z), \wp'(z))$. Choose $\Omega \in L$ such that $L = \Omega\mathcal{O}$. We identify $\mathcal{O}$ with the endomorphism ring of E in such a way that the endomorphism corresponding to $\alpha \in \mathcal{O}$ is given by $\xi(z) \mapsto \xi(\alpha z)$. If $\alpha \in \mathcal{O}$, we write E_α for the kernel of the endomorphism α of E. Let ψ be the Grössencharacter of E over K as defined in [7], §7.8. We denote the conductor of ψ by $\mathfrak{f}$, and write f for some fixed generator of $\mathfrak{f}$.

Let F be an arbitrary finite abelian extension of K, which will be fixed for the rest of the paper. We write S for the finite set consisting of 2, 3, and all rational primes q which have a prime factor in K, which is either ramified in F, or at which E has a bad reduction. Henceforth, p will denote a rational prime, which splits in K, and which does not belong to the finite exceptional set S. We write $\wp$ and $\bar{\wp}$ for the factors of p in K, and put $\pi = \psi(\wp)$. Thus, by the definition of ψ, π is a generator of the ideal $\wp$. Finally, let $\mathfrak{g}$ denote the least common multiple of the conductor of ψ and the conductor of F/K.

2. Computation of conductors

We now compute the conductors of various abelian extensions of K which occur in the proof of Theorem 1. The arguments are similar to those in §2 of [4]. If $\alpha \in \mathcal{O}$, recall that E_α is the group of α-division points on E.

LEMMA 2: *Let $\mathfrak{h} = (h)$ be any multiple of the conductor of ψ. Then $K(E_h)$ is the ray class field of K modulo $\mathfrak{h}$.*

PROOF: By the classical theory of complex multiplication, the ray class field modulo $\mathfrak{h}$ is contained in $K(E_h)$. To prove the converse, we use the notation and results of Shimura [7]. Let $U(\mathfrak{h})$ be the subgroup of the idèle group of K as defined on p. 116 of [7], and let x be any element of $U(\mathfrak{h})$ with $x_\infty = 1$. Since the conductor of ψ divides $\mathfrak{h}$, it follows from Shimura's reciprocity law (cf. the proof of Lemma 3 in [4]) that the Artin symbol $[x, K]$ fixes E_h. Thus $K(E_h)$ is contained in the ray class field modulo $\mathfrak{h}$, and the proof of the lemma is complete.

Recall that $\mathfrak{g}$ is the least common multiple of the conductor of ψ, and the conductor of F/K. Also, p is any rational prime, not in S, which splits in K, say $(p) = \wp\bar{\wp}$.

LEMMA 3: *For each $n \geq 0$, the conductor of $F_n = F(E_{\pi^{n+1}})$ over K is equal to $\mathfrak{f}_n = \mathfrak{g}\wp^{n+1}$. Moreover, if $\mathfrak{R}_n$ denotes the ray class field of K modulo $\mathfrak{f}_n$, then $\mathfrak{R}_n$ is the compositum of F_n and $H = K(E_g)$, and $F_n \cap H = F$.*

PROOF: Let $\mathfrak{g}_n$ denote the conductor of F_n/K. Since $F_n \subset K(E_{g\pi^{n+1}})$, and the conductor of this latter field is $\mathfrak{f}_n = \mathfrak{g}\wp^{n+1}$ by Lemma 2, we conclude that $\mathfrak{g}_n$ divides $\mathfrak{f}_n$. On the other hand, it is clear that the conductor of F over K divides $\mathfrak{g}_n$. Also, as E has a good reduction everywhere over F_n (see Theorem 2 of [4]), the Grössencharacter of E over F_n must be unramified. As the Grössencharacter of E over F_n is the composition of the norm map from F_n to K with ψ, it follows that the conductor $\mathfrak{f}$ of ψ divides $\mathfrak{g}_n$. Combining these last two facts, we conclude that $\mathfrak{g}$ divides $\mathfrak{g}_n$. But $\wp^{n+1}$ divides $\mathfrak{g}_n$ because F_n contains the ray class field modulo $\wp^{n+1}$. As $(\wp, \mathfrak{g}) = 1$ by hypothesis, we deduce that $\mathfrak{g}_n = \mathfrak{f}_n$, as asserted. To prove the final statement of the lemma, we recall that $\mathcal{R}_n = K(E_{\mathfrak{g}\pi^{n+1}})$ by Lemma 2, and thus $\mathcal{R}_n$ is certainly the compositum of F_n and H. Now $\wp$ is totally ramified in $K(E_{\pi^{n+1}})$ by the rudiments of Lubin-Tate theory. As $\wp$ does not divide the conductor of F over K, it follows that each prime of F above $\wp$ is totally ramified in F_n. Since $\wp$ does not divide $\mathfrak{g}$ by hypothesis, and H is the ray class field modulo $\mathfrak{g}$ by Lemma 2, we deduce that $F_n \cap H = F$, as required.

3. p-Adic logarithmic derivatives

We use the same notation as [4] for the formal groups $\hat{E}$ and $\mathscr{E}$. Thus $\hat{E}$ is the formal group giving the kernel of reduction modulo $\wp$ on E, and $\mathscr{E}$ is the Lubin-Tate formal group for which $[\pi](w) = \pi w + w^p$. By Lubin-Tate theory, $\hat{E}$ and $\mathscr{E}$ are isomorphic over the ring $\mathcal{O}_\wp$ of integers of the completion $K_\wp$ of K at $\wp$. For a fuller discussion, see §3 of [4].

Choose a fixed algebraic closure $\bar{K}_\wp$ of $K_\wp$. We can assume that E_π lies in $\bar{K}_\wp$, and we define the extension Φ of $K_\wp$ by

$$\Phi = K_\wp(E_\pi) = K_\wp(\mathscr{E}_\pi).$$

Put $G = G(\Phi/K_\wp)$. Of course, G is endowed with the canonical character χ, with values in $Z_p^\times$, giving the action of G on E_π, or equivalently, on $\mathscr{E}_\pi$. Thus, if A is any $\mathbf{Z}_p[G]$-module, it has a canonical decomposition

$$A = \bigoplus_{k=1}^{p-1} A^{(k)}, \tag{2}$$

where $A^{(k)}$ is the submodule of A on which G acts via the k-th power of χ.

Let u be a fixed generator for $\mathscr{E}_\pi$, so that u is a local parameter for Φ. Let U be the group of units of Φ which are $\equiv 1 \bmod u$. For $1 \le k \le p-2$, we define homomorphisms

$$\varphi_k : U \to \mathcal{O}_\wp/\wp \tag{3}$$

as follows. If $\alpha \in U$, we choose any power series $f(T) = \Sigma_{k=0}^{\infty} a_k T^k$, with $a_k \in \mathcal{O}_\wp$, such that $f(u) = \alpha$. We then define $\varphi_k(\alpha)$ to be the residue class in $\mathcal{O}_\wp/\wp$ of the coefficient of T^k in the power series $T(\mathrm{d}/\mathrm{d}T)\log f(T)$. Since $1 \le k \le p-2$ and the ramification index of Φ over $K_\wp$ is $p-1$, it is easy to see that $\varphi_k(\alpha)$ is independent of the choice of $f(T)$, and so is well defined.

REMARK: In defining φ_k in [4], one insisted that the power series $f(T)$ had $a_0 = 1$. It is more convenient for the arguments in §4 to work with power series whose constant term is not necessarily 1. Of course, the two definitions of φ_k are the same for $1 \le k \le p-2$. However, one cannot define φ_{p-1} by the present method.

In the proof of Theorem 1, we shall only be interested in the case in which Φ contains no non-trivial p-power roots of unity. Recall that, by Lemma 12 of [4], if $p > 5$, then Φ can contain a non-trivial p-th root of unity if and only if $\pi + \bar{\pi} = 1$. The next lemma is plain from Lemmas 9 and 10 of [4].

LEMMA 4: *Assume that Φ contains no non-trivial p-th root of unity. Let k be an integer with $1 \le k \le p-2$. Then φ_k vanishes on $U^{(j)}$ for $j \not\equiv k \bmod (p-1)$, and φ_k induces an isomorphism*

$$\tilde{\varphi}_k : U_0^{(k)}/(U_0^{(k)})^p \xrightarrow{\sim} \mathcal{O}_\wp/\wp.$$

Now consider our fixed finite abelian extension F of K, and $F_0 = F(E_\pi)$. Let $\mathcal{S}$ be the set of primes of F_0 above $\wp$. For each $\mathfrak{q} \in \mathcal{S}$, let $F_{0,\mathfrak{q}}$ be the completion of F_0 at $\mathfrak{q}$, and write $U_\mathfrak{q}$ for the units in $F_{0,\mathfrak{q}}$ which are $\equiv 1 \bmod \mathfrak{q}$. Put

$$\mathcal{U} = \prod_{\mathfrak{q} \in \mathcal{S}} U_\mathfrak{q}. \tag{4}$$

Now assume that $\wp$ splits completely in F. Thus, for each $\mathfrak{q} \in \mathcal{S}$, there exists an isomorphism $\tau_\mathfrak{q} : F_{0,\mathfrak{q}} \xrightarrow{\sim} \Phi$, which preserves the valuations of both fields. Composing this isomorphism with the map φ_k given by (3), we obtain a homomorphism

$$\varphi_{\mathfrak{q},k} : U_\mathfrak{q} \to \mathcal{O}_\wp/\wp \qquad (1 \le k \le p-2). \tag{5}$$

We define

$$\varphi_{F,k} : \mathcal{U} \to \prod_{\mathfrak{q} \in \mathcal{S}} (\mathcal{O}_\wp/\wp) \tag{6}$$

to be the product of the homomorphisms (5) over all $\mathfrak{q} \in \mathcal{S}$. Plainly $G = G(F_0/F) = G(\Phi/K_\wp)$ acts on (4), because it acts on each of the $U_\mathfrak{q}$ in the natural way. The next lemma is now plain from Lemma 4.

LEMMA 5: *Assume that Φ contains no non-trivial p-th root of unity, and that $\wp$ splits completely in F. Let k be an integer with $1 \leq k \leq p-2$. Then $\varphi_{F,k}$ vanishes on $\mathcal{U}^{(j)}$ for $j \not\equiv k \bmod(p-1)$, and $\varphi_{F,k}$ induces an isomorphism*

$$\widetilde{\varphi_{F,k}}: \mathcal{U}^{(k)}/(\mathcal{U}^{(k)})^p \xrightarrow{\sim} \prod_{\mathfrak{q} \in \mathcal{S}} (\mathcal{O}_\wp/\wp).$$

Put $d = [F:K]$. In practice, we shall use the following immediate consequence of Lemma 5.

COROLLARY 6: *Under the same hypotheses as Lemma 5, let A be any $\mathbf{Z}_p[G]$-submodule of $\mathcal{U}$. Then, for each integer k with $1 \leq k \leq p-2$, the eigenspace $(\mathcal{U}/A)^{(k)} \neq 0$ if and only if $\varphi_{F,k}(A)$ has dimension less than d over the field $\mathcal{O}_\wp/\wp$.*

4. Elliptic units

As in [4], a vital role in the proof of Theorem 1 is played by the elliptic units of Robert [6]. We begin by briefly recalling the definition of these elliptic units. Let $\mathcal{I}$ be the set consisting of all pairs $(A, \mathcal{N})$, where $A = \{\mathfrak{a}_j : j \in J\}$ and $\mathcal{N} = \{n_j : j \in J\}$, here J is an arbitrary finite index set, the $\mathfrak{a}_j$ are integral ideals of K prime to S and p, and the n_j are rational integers satisfying $\Sigma_{j \in J}\, n_j(N\mathfrak{a}_j - 1) = 0$. Given such a pair $(A, \mathcal{N})$, we put

$$\Theta(z, A, \mathcal{N}) = \prod_{j \in J} \Theta(z, \mathfrak{a}_j)^{n_j},$$

where $\Theta(z, \mathfrak{a}_j)$ is as defined at the beginning of §4 of [4]. Recall that $\mathfrak{f}_n = \mathfrak{g}\wp^{n+1}$ is the conductor of $F_n = F(E_{\pi^{n+1}})$ over K. As before, let $\mathcal{R}_n$ be the ray class field of K modulo $\mathfrak{f}_n$. If ρ_n is an arbitrary primitive $\mathfrak{f}_n$-division point of L, Robert [6] has shown that $\Theta(\rho_n, A, \mathcal{N})$ is a unit of the field $\mathcal{R}_n$. Moreover, as $(A, \mathcal{N})$ ranges over $\mathcal{I}$, the $\Theta(\rho_n, A, \mathcal{N})$ form a subgroup of the group of units of $\mathcal{R}_n$. We denote this subgroup by $\mathcal{C}_n$, and call it the group of elliptic units of $\mathcal{R}_n$ (note that Robert's definition of the group of elliptic units is different from ours). A similar argument to that given in the proof of Lemma 20 of [4] shows that $\mathscr{C}_n$ is stable under the action of the Galois group of $\mathscr{R}_n$ over K, and is independent of the choice of the particular primitive $\mathfrak{f}_n$-division point ρ_n. Finally, we define the elliptic units C_n of $F_n = F(E_{\pi^{n+1}})$ to be the group consisting of the norms from $\mathscr{R}_n$ to F_n of all units in $\mathscr{C}_n$. For simplicity, we often write C for C_0.

Let $\rho = \Omega/g$, where $\mathfrak{q} = (g)$. Here $L = \Omega\mathcal{O}$ is the period lattice of $\wp(z)$. As above, let $\mathscr{R}_0$ be the ray class field of K modulo $\mathfrak{f}_0 = \mathfrak{g}\mathfrak{p}$. Lemma 3 tells us that we have the diagram of fields

$$
(7)\qquad
\begin{array}{ccccc}
 & & \mathscr{R}_0 = HF_0 & & \\
 & \diagup & & \diagdown & \\
H = K(E_g) & & & & F_0 = F(E_\pi) \\
 & \diagdown & & \diagup & \\
 & & F = H \cap F_0 & & \\
 & & | & & \\
 & & K & &
\end{array}
$$

If L is any finite abelian extension of K, and $\mathfrak{c}$ is an integral ideal of K prime to the conductor of L/K, we write $(\mathfrak{c}, L/K)$ for the Artin symbol of $\mathfrak{c}$ for the extension L/K. We now choose and fix a set B of integral ideals of K, which are prime to $\mathfrak{f}_0$, and which are such that $\{(\mathfrak{b}, \mathscr{R}_0/K) : \mathfrak{b} \in B\}$ is precisely the Galois group of $\mathscr{R}_0/F_0$. It is then plain from (7) that the restrictions of the $(\mathfrak{b}, \mathscr{R}_0/K)$, $\mathfrak{b} \in B$, to H is precisely the Galois group of H/F.

If $\mathfrak{a}$ is an arbitrary integral ideal of K prime to S and p, we define

$$\Lambda(z, \mathfrak{a}) = \prod_{\mathfrak{b} \in B} \Theta(z + \psi(\mathfrak{b})\rho, \mathfrak{a}).$$

Lemma 7: *$\Lambda(z, \mathfrak{a})$ is a rational function of $\wp(z)$ and $\wp'(z)$ with coefficients in F.*

Proof: This is entirely similar to the first part of the proof of Lemma 21 of [4], and so we omit it.

It is now convenient to introduce some notation, which will be used repeatedly in this section. Let $\mathscr{G}$ denote the Galois group of F over K. If $\mathfrak{c}$ is an integral ideal of K prime to the conductor of F/K, we write $\sigma_\mathfrak{c}$ for the Artin symbol $(\mathfrak{c}, F/K)$. Finally, if $\sigma \in \mathscr{G}$ and $R(z)$ is a rational function of $\wp(z)$, $\wp'(z)$ with coefficients in F, then $R_\sigma(z)$ will denote the rational function of $\wp(z)$, $\wp'(z)$, which is obtained by letting σ act on the coefficients of $R(z)$.

Let k be an integer ≥ 1. Recall that ψ denotes the Grössencharacter of E. For each $\sigma \in \mathcal{G}$, we introduce the partial Hecke L-function

$$\zeta_F(\sigma, k; s) = \sum_{\substack{(\mathfrak{a},\mathfrak{g})=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \frac{\bar{\psi}^k(\mathfrak{a})}{(N\mathfrak{a})^s},$$

where the summation is over all integral ideals $\mathfrak{a}$ of K, prime to $\mathfrak{g}$, such that the Artin symbol $\sigma_{\mathfrak{a}}$ is equal to σ. It can be shown that $\zeta_F(\sigma, k; s)$ can be analytically continued over the whole complex plane. Let $\zeta_F(\sigma, k)$ denote the value of $\zeta_F(\sigma, k; s)$ at $s = k$.

LEMMA 8: *For each* $\sigma \in \mathcal{G}$, *we have*

$$z\frac{\mathrm{d}}{\mathrm{d}z}\log \Lambda_\sigma(z, \mathfrak{a}) = \sum_{k=1}^{\infty} c_k(\mathfrak{a}, \sigma)z^k, \quad \textit{where}$$

$$c_k(\mathfrak{a}, \sigma) = 12(-1)^{k-1}\rho^{-k}(N\mathfrak{a}\zeta_F(\sigma, k) - \psi^k(\mathfrak{a})\zeta_F(\sigma\sigma_{\mathfrak{a}}, k)) \qquad (k = 1, 2, \ldots).$$

PROOF: Let $\mathfrak{c}$ be an integral ideal of K, prime to $\mathfrak{g}$, such that $\sigma = \sigma_{\mathfrak{c}}$. By the definition of the Grössencharacter ψ in [7], we have

$$\xi(\psi(\mathfrak{b})\rho)^{(\mathfrak{c},H/K)} = \xi(\psi(\mathfrak{b}\mathfrak{c})\rho).$$

It follows easily from the expression for $\Theta(z + \psi(\mathfrak{b})\rho, \mathfrak{a})$ as a rational function of $\wp(z), \wp'(z)$, with coefficients in H (see (23) of [4]), that

$$\Lambda_\sigma(z, \mathfrak{a}) = \prod_{\mathfrak{b}\in B} \Theta(z + \psi(\mathfrak{b}\mathfrak{c})\rho, \mathfrak{a}).$$

If $\mathcal{L}$ is any lattice in the complex plane, let $\zeta(z, \mathcal{L})$ and $\wp(z, \mathcal{L})$ be the Weierstrass zeta and $\wp$-functions of $\mathcal{L}$. Define

$$\Omega(z, \mathcal{L}) = z\frac{\mathrm{d}}{\mathrm{d}z}\log\Big(\prod_{\mathfrak{b}\in B} \theta(z + \psi(\mathfrak{b}\mathfrak{c})\rho, \mathcal{L})\Big).$$

Then (cf. the proof of Lemma 21 of [4]) $\Omega(z, \mathcal{L})$ has the power series expansion $\Sigma_{k=1}^{\infty} d_k(\mathcal{L})z^k$, where $\eta = \psi(\mathfrak{c})\rho$ and

(8) $$d_1(\mathcal{L}) = 12\sum_{\mathfrak{b}\in B} (\zeta(\psi(\mathfrak{b})\eta, \mathcal{L}) - s_2(\mathcal{L})\psi(\mathfrak{b})\eta),$$

(9) $$d_2(\mathcal{L}) = -12\sum_{\mathfrak{b}\in B} (\wp(\psi(\mathfrak{b})\eta, \mathcal{L}) + s_2(\mathcal{L})),$$

(10) $$d_k(\mathcal{L}) = -12\sum_{\mathfrak{b}\in B} \wp^{(k-2)}(\psi(\mathfrak{b})\eta, \mathcal{L})/(k-1)! \quad (k \geq 3).$$

Thus we must show that $c_k(\mathfrak{a}, \sigma)$, as defined in Lemma 8, satisfies

$$c_k(\mathfrak{a}, \sigma) = N\mathfrak{a}\, d_k(L) - d_k(\mathfrak{a}^{-1}L) \qquad (k \geq 1). \tag{11}$$

As in [4], we put $\lambda_k = 12(-1)^{k-1}\rho^{-k}$. We write $\mathscr{B}$ for a fixed set of generators of the ideals in B. Also, we let γ denote a fixed generator of the ideal $\mathfrak{a}$, and c a fixed generator of $\mathfrak{c}$. The argument now breaks up into three cases. Much of the reasoning is similar to that in the proof of Lemma 21 of [4], so that we refer there for details from time to time.

Case 1. We suppose that $k \geq 3$. Since

$$\wp^{(k-2)}(z, \mathscr{L}) = (-1)^k (k-1)! \sum_{\omega \in \mathscr{L}} (z-\omega)^{-k} \quad (k \geq 3),$$

we conclude easily from (10) that

$$d_k(L) = \lambda_k \sum_{\mathfrak{b} \in B} \sum_{\alpha \in \mathfrak{g}} (\psi(\mathfrak{bc}) - \alpha)^{-k}.$$

We now write $\psi(\mathfrak{bc}) = \epsilon(bc)bc$, where b is the generator of $\mathfrak{b}$ in $\mathscr{B}$, and $\epsilon(bc)$ is a root of unity in K, and argue in exactly the same way as in Case 1 of the proof of Lemma 21 in [4]. In this way, it follows that

$$d_k(L) = \lambda_k \sum_{b \in \mathscr{B}} \sum_{\alpha \in \mathfrak{g}} \bar{\psi}^k((bc - \alpha)) N(bc - \alpha)^{-k},$$

where N denotes the norm from K to $\mathbf{Q}$. Let W denote the group of roots of unity of K. Since the Grössencharacter ψ is defined modulo $\mathfrak{g}$, the natural map of W into $(\mathcal{O}/\mathfrak{g})^\times$ is plainly injective. Now, as H is the ray class field modulo $\mathfrak{g}$ by Lemma 2, we can identify the Galois group of H over K with $(\mathcal{O}/\mathfrak{g})^\times/W$ via the Artin map. Since the Artin symbol of $\mathfrak{c} = (c)$ for F/K is equal to σ, it is therefore clear that $\{\mu bc : \mu \in W, b \in \mathscr{B}\}$ is a complete set of representatives of those elements in $(\mathcal{O}/\mathfrak{g})^\times$, whose Artin symbol has restriction to F equal to σ. In other words,

$$\{\mu bc - \alpha : \mu \in W, b \in \mathscr{B}, \alpha \in \mathfrak{g}\}$$

is the set of all algebraic integers in K, prime to $\mathfrak{g}$, such that the Artin symbol for F/K of the associated principal ideal is equal to σ. Since we can plainly rewrite the above expression for $d_k(L)$ as

$$d_k(L) = \frac{\lambda_k}{w_k} \sum_{\mu \in W} \sum_{b \in \mathscr{B}} \sum_{\alpha \in \mathfrak{g}} \bar{\psi}^k((\mu bc - \alpha)) N(\mu bc - \alpha)^{-k},$$

where w_k denotes the number of roots of unity in K, it follows that

$$d_k(L) = \lambda_k \zeta_F(\sigma, k).$$

Now consider $d_k(\mathfrak{a}^{-1}L)$. Recalling that $\mathfrak{a} = (\gamma)$, it follows from (10) that

$$d_k(\mathfrak{a}^{-1}L) = \lambda_k \gamma^k \sum_{\mathfrak{b} \in B} \sum_{\alpha \in \mathfrak{g}} (\gamma\psi(\mathfrak{b}\mathfrak{c}) - \alpha)^{-k}.$$

Substitute $\gamma = \psi(\mathfrak{a})\epsilon^{-1}(\gamma)$ for the first occurrence of γ on the right hand side of this equation. Again arguing in the same way as in Case 1 of the proof of Lemma 21 in [4], we obtain

$$d_k(\mathfrak{a}^{-1}L) = \lambda_k \psi^k(\mathfrak{a}) \sum_{b \in \mathscr{B}} \sum_{\alpha \in \mathfrak{g}} \bar{\psi}^k((\gamma bc - \alpha)) N(\gamma bc - \alpha)^{-k}.$$

Now

$$\{\mu\gamma bc - \alpha : \mu \in W,\ b \in \mathscr{B},\ \alpha \in \mathfrak{g}\}$$

is the set of all algebraic integers in K, prime to $\mathfrak{g}$, such that the Artin symbol for F/K of the associated principal ideal is equal to $\sigma\sigma_{\mathfrak{a}}$. Thus

$$d_k(\mathfrak{a}^{-1}L) = \lambda_k \psi^k(\mathfrak{a}) \zeta_F(\sigma\sigma_{\mathfrak{a}}, k).$$

We have therefore proven (11) in this case.

Case 2. We assume that $k = 2$. Now, for any lattice $\mathscr{L}$,

$$\wp(z, \mathscr{L}) = \lim_{\substack{s \to 0 \\ s > 0}} \sum_{\omega \in \mathscr{L}} (z - \omega)^{-2} |z - \omega|^{-2s} - s_2(\mathscr{L}),$$

where $s_2(\mathscr{L})$ is as defined at the beginning of §4 of [4]. Taking $\mathscr{L} = L$, we deduce from (9) that

$$d_2(L) = \lambda_2 \lim_{\substack{s \to 0 \\ s > 0}} \sum_{\mathfrak{b} \in B} \sum_{\alpha \in \mathfrak{g}} (\psi(\mathfrak{b}\mathfrak{c}) - \alpha)^{-2} |\psi(\mathfrak{b}\mathfrak{c}) - \alpha|^{-2s}.$$

Arguing as in the previous case, we obtain $d_2(L) = \lambda_2\zeta_F(\sigma, 2)$. Similarly, $d_2(\mathfrak{a}^{-1}L) = \lambda_2\psi^2(\mathfrak{a})\zeta_F(\sigma\sigma_{\mathfrak{a}}, 2)$, and so we obtain (11) in this case.

Case 3. We assume that $k = 1$. If $\mathscr{L}$ is any lattice, let $H(s, z, \mathscr{L})$ denote the analytic continuation in s of the series

$$\sum_{\omega\in\mathscr{L}} (\bar{z} + \bar{\omega})|z + \omega|^{-2s}$$

(this series converges for $R(s) > 3/2$). Then, as is shown in case 3 of the proof of Lemma 21 of [4], we have

$$\zeta(z, \mathscr{L}) - zs_2(\mathscr{L}) = H(1, z, \mathscr{L}) + \bar{z}g(\mathscr{L}),$$

where $g(\mathscr{L})$ is defined in the same proof. First take $\mathscr{L} = L$. It follows from (8) that

$$d_1(L) = \lambda_1 \lim_{s\to 1} \sum_{\mathfrak{b}\in B} \sum_{\alpha\in\mathfrak{q}} \frac{\bar{\psi}(\mathfrak{b}\mathfrak{c}) + \bar{\alpha}}{|\psi(\mathfrak{b}\mathfrak{c}) + \alpha|^{2s}} + rg(L),$$

where $r = \Sigma_{\mathfrak{b}\in B} (\bar{\psi}(\mathfrak{b}\mathfrak{c})\bar{\rho})$ (here, by the limit as $s \to 1$, we mean the value of the analytic continuation at $s = 1$). As before, we deduce easily that

$$d_1(L) = \lambda_1\zeta_F(\sigma, 1) + rg(L).$$

Next take $\mathscr{L} = \gamma^{-1}L$. Then

$$d_1(\mathfrak{a}^{-1}L) = \lambda_1 \lim_{s\to 1} \sum_{\mathfrak{b}\in B} \sum_{\alpha\in\gamma^{-1}\mathfrak{q}} \frac{\bar{\psi}(\mathfrak{b}\mathfrak{c}) + \bar{\alpha}}{|\psi(\mathfrak{b}\mathfrak{c}) + \alpha|^{2s}} + rg(\gamma^{-1}L).$$

Taking the factor γ^{-1} out of each α, and recalling that $g(\gamma^{-1}L) = N\mathfrak{a}g(L)$, we conclude that

$$d_1(\mathfrak{a}^{-1}L) = \lambda_1\gamma \lim_{s\to 1} \sum_{\mathfrak{b}\in B} \sum_{\alpha\in\mathfrak{q}} \frac{\bar{\gamma}\bar{\psi}(\mathfrak{b}\mathfrak{c}) + \bar{\alpha}}{|\gamma\psi(\mathfrak{b}\mathfrak{c}) + \alpha|^{2s}} + rN\mathfrak{a}g(L).$$

We now argue in the same way as in case 1 to deduce that

$$d_1(\mathfrak{a}^{-1}L) = \lambda_1\psi(\mathfrak{a})\zeta_F(\sigma\sigma_{\mathfrak{a}}, 1) + rN\mathfrak{a}g(L).$$

Combining these two expressions for $d_1(L)$ and $d_1(\mathfrak{a}^{-1}L)$, we see that (11) is true for $k = 1$. This completes the proof of Lemma 8.

Corollary 9: *For each integer $k \geq 1$, and each $\sigma \in \mathscr{G}$, $\Omega^{-k}\zeta_F(\sigma, k)$ belongs to F. Moreover, if $\tau \in \mathscr{G}$, then $(\Omega^{-k}\zeta_F(\sigma, k))^\tau = \Omega^{-k}\zeta_F(\tau\sigma, k)$.*

Proof: The first assertion is plain from Lemmas 7 and 8, on taking $\mathfrak{a} \neq 1$ to be an integral ideal of K, prime to S and p, such that $\sigma_{\mathfrak{a}} = 1$. The second assertion follows similarly, on noting that $c_k(\mathfrak{a}, \sigma)^\tau = c_k(\mathfrak{a}, \tau\sigma)$ for all $k \geq 1$ because $\Lambda_\sigma(z, \mathfrak{a})^\tau = \Lambda_{\tau\sigma}(z, \mathfrak{a})$. Here $\Lambda_\sigma(z, \mathfrak{a})^\tau$ denotes the rational function of $\wp(z)$ and $\wp'(z)$, with coefficients in F, which is obtained by letting τ act on the coefficients of $\Lambda_\sigma(z, \mathfrak{a})$.

Let ψ_F denote the Grössencharacter of F, which is obtained by composing ψ with the norm map from F to K. Plainly ψ_F is unramified outside $\mathfrak{g}$. Thus, for each integer $k \geq 1$, we can define

$$L_F(\bar{\psi}_F^k, s) = \prod_{(\mathfrak{P}, \mathfrak{g})=1} (1 - \bar{\psi}_F^k(\mathfrak{P})(N\mathfrak{P})^{-s})^{-1},$$

the product being taken over all primes $\mathfrak{P}$ of F which do not divide $\mathfrak{g}$. Of course, $L_F(\bar{\psi}_F^k, s)$ will not, in general, be a primitive Hecke L-function, but this will not be important in the proof of Theorem 1. Let $\hat{\mathscr{G}}$ denote the group of all homomorphisms from $\mathscr{G}$ into the group of non-zero complex numbers. If $\theta \in \hat{\mathscr{G}}$, we associate with it the complex L-function

$$L_F(\bar{\psi}^k\theta, s) = \sum_{\sigma \in \mathscr{G}} \theta(\sigma)\zeta_F(\sigma, k; s).$$

One verifies immediately that we have the product decomposition

$$L_F(\bar{\psi}_F^k, s) = \prod_{\theta \in \hat{\mathscr{G}}} L_F(\bar{\psi}^k\theta, s). \tag{12}$$

The next lemma gives the basic rationality properties of the value of $L_F(\bar{\psi}_F^k, s)$ at $s = k$.

Lemma 10: *For each integer $k \geq 1$, $\Omega^{-kd}L_F(\bar{\psi}_F^k, k)$ belongs to F, and the ideal that it generates is fixed by the action of $\mathscr{G}$.*

Proof: By (12) and the first assertion of Corollary 9, we see that $\nu_k = \Omega^{-kd}L_F(\bar{\psi}_F^k, k)$ belongs to M, where M is the field obtained by adjoining to F the values of all $\theta \in \hat{\mathscr{G}}$. But, again by (12), it is clear that ν_k is fixed by the Galois group of M over F, and so belongs to F. Now take τ to be any element of $\mathscr{G}$, and let τ_1 be an element of $G(M/K)$ whose restriction to F is τ. The second assertion of Corollary 9 implies that

$$\Omega^{-k}L_F(\bar{\psi}^k\theta, k)^{\tau_1} = \theta^{\tau_1}(\tau^{-1})\Omega^{-k}L_F(\bar{\psi}^k\theta^{\tau_1}, k), \tag{13}$$

whence it is plain from (12) that the ideal in F generated by ν_k is fixed by $\mathcal{G}$.

REMARK: If $\mathcal{G}$ has no quadratic characters, (12) and (13) show that $\Omega^{-kd}L_F(\bar{\psi}_F^k, k)$ is actually fixed by $\mathcal{G}$, and so belongs to K.

We now investigate the integrality properties of the numbers in Corollary 9 and Lemma 10. Let $\mathfrak{P}$ be any prime of F lying above $\wp$, $F_{\mathfrak{P}}$ the completion of F at $\mathfrak{P}$, and $\mathcal{O}_{\mathfrak{P}}$ the ring of integers of $F_{\mathfrak{P}}$. We can view $\Lambda_\sigma(z, \mathfrak{a})$ as being a rational function of $\wp(z)$ and $\wp'(z)$ with coefficients in $F_{\mathfrak{P}}$, via the canonical inclusion of F in $F_{\mathfrak{P}}$. Hence we can expand $\Lambda_\sigma(z, \mathfrak{a})$ in terms of the parameter $t = -2\wp(z)/\wp'(z)$ of the formal group $\hat{E}$.

LEMMA 11: *Let $\mathfrak{P}$ be any prime of F above $\wp$. In terms of the parameter $t = -2\wp(z)/\wp'(z)$, $\Lambda_\sigma(z, \mathfrak{a})$ has an expansion*

$$\Lambda_\sigma(z, \mathfrak{a}) = \sum_{k=0}^{\infty} h_{k,\sigma}(\mathfrak{a}, \mathfrak{P})t^k,$$

whose coefficients all belong to $\mathcal{O}_{\mathfrak{P}}$, and where $h_{0,\sigma}(\mathfrak{a}, \mathfrak{P})$ is a unit in $\mathcal{O}_{\mathfrak{P}}$.

PROOF: This is the same as the proof of Lemma 23 of [4] (on recalling that $(\mathfrak{g}, \wp) = 1$ by hypothesis), and so we omit the details.

LEMMA 12: *Let k be an integer with $1 \leq k \leq p-1$. Then* (i) *for $\sigma \in \mathcal{G}$, $\Omega^{-k}\zeta_F(\sigma, k)$ is integral at each prime of F above $\wp$, and* (ii) *$\Omega^{-kd}L_F(\bar{\psi}_F^k, k)$ is integral at each prime of F above $\wp$.*

PROOF: In view of (12), it is plain that (ii) is a consequence of (i). We now proceed to deduce (i) from the previous lemma. Let w be the parameter of the Lubin-Tate formal group $\mathcal{E}$ such that $[\pi](w) = \pi w + w^p$ (cf. §3 of [4]). Fix a prime $\mathfrak{P}$ of F above $\wp$. For the moment, take $\mathfrak{a}$ to be an arbitrary integral ideal of K, prime to S and p. Since t can be written as a power series in w with coefficients in $\mathcal{O}_\wp$, it follows from Lemma 11 that $\Lambda_\sigma(z, \mathfrak{a})$ can be expanded as a power series in w, say $f(w)$, with coefficients in $\mathcal{O}_{\mathfrak{P}}$, and whose constant term $f(0)$ is a unit in $\mathcal{O}_{\mathfrak{P}}$. Moreover, since $z = w + \sum_{i=2}^{\infty} a_i w^i$, where $a_i = 0$ unless

$i \equiv 1 \bmod (p-1)$ (cf. Lemma 7 of [4]), the coefficients of z^k and w^k $(0 \le k \le p-1)$ in the z-expansion of $\Lambda_\sigma(z, \mathfrak{a})$ and in $f(w)$ are plainly equal. It follows that the coefficients of z^k and w^k $(1 \le k \le p-1)$ in the z-expansion of $z(\mathrm{d}/\mathrm{d}z)\log \Lambda_\sigma(z, \mathfrak{a})$ and in $w(\mathrm{d}/\mathrm{d}w)\log f(w)$ are also equal. But the coefficients of this latter series lie in $\mathcal{O}_{\mathfrak{P}}$, because the constant term $f(0)$ of $f(w)$ is a unit in $\mathcal{O}_{\mathfrak{P}}$. We conclude from Lemma 8 that

$$\Omega^{-k}(N\mathfrak{a}\zeta_F(\sigma, k) - \psi^k(\mathfrak{a})\zeta_F(\sigma\sigma_{\mathfrak{a}}, k)) \tag{14}$$

is integral at $\mathfrak{P}$ for $1 \le k \le p-1$. We now make a special choice of the ideal $\mathfrak{a}$. Let e denote a generator of the ideal $(12g) \cap \mathbb{Z}$. Choose n to be a rational integer, prime to p, such that $1 + ne\pi$ is not divisible by $\bar{\wp}$, and take $\mathfrak{a} = (1 + ne\,\pi)$. Then $N\mathfrak{a} \equiv 1 \bmod \wp$. Also $\sigma_{\mathfrak{a}} = 1$ because the conductor of F/K divides e, and $\psi^k(\mathfrak{a}) = (1 + en\pi)^k \equiv 1 \bmod \wp$, because the conductor of ψ divides e. Thus $N\mathfrak{a} - \psi^k(\mathfrak{a})$ is a unit at $\wp$, and so assertion (i) follows from (14). This completes the proof of Lemma 12.

We now prove a technical lemma, which establishes the existence of d pairs $(A, \mathcal{N})$ in $\mathcal{I}$, with properties which will be needed later in this section. To simplify the statement of the lemma, we choose a fixed numbering of the elements of $\mathcal{G}$, say $\sigma_1, \ldots, \sigma_d$, with $\sigma_1 = 1$.

LEMMA 13: *Let k be an integer with $1 \le k \le p-2$. Then there exist d pairs $(A^{(h)}, \mathcal{N}^{(h)}) \in \mathcal{I}$, where*

$$A^{(h)} = \{\mathfrak{a}_1^{(h)}, \mathfrak{a}_2^{(h)}\}, \quad \mathcal{N}^{(h)} = \{n_1^{(h)}, n_2^{(h)}\} \qquad (1 \le h \le d),$$

with the following properties. Firstly, $\psi^k(\mathfrak{a}_2^{(1)}) \not\equiv 1 \bmod \wp$. Secondly, for $1 \le h \le d$, we have (i) $\psi^k(\mathfrak{a}_1^{(h)}) \equiv 1 \bmod \wp$, (ii) $\sigma_{\mathfrak{a}_2^{(h)}} = 1$, (iii) $\sigma_{\mathfrak{a}_1^{(h)}} = \sigma_h^{-1}$, *and* (iv) *$n_2^{(h)}$ is prime to p.*

PROOF: Let e denote a generator of the ideal $(12g) \cap \mathbb{Z}$, and let $\beta \bmod \wp$ be a generator of $(\mathcal{O}/\wp)^\times$. First consider the case $h = 1$. Let n be a rational integer, prime to p, such that $1 + ne\pi$ is prime to $\bar{\wp}$, and take $\mathfrak{a}_1^{(1)} = (1 + en\pi)$. Choose $\mathfrak{a}_2^{(1)} = (\alpha_2^{(1)})$, where $\alpha_2^{(1)}$ is an algebraic integer in K satisfying $\alpha_2^{(1)} \equiv 1 \bmod e\bar{\pi}$, and $\alpha_2^{(1)} \equiv \beta \bmod \pi$. Let $n_1^{(1)} = N\mathfrak{a}_2^{(1)} - 1$ and $n_2^{(1)} = -(N\mathfrak{a}_1^{(1)} - 1)$, so that $n_2^{(1)}$ is prime to p because $(p, ne) = 1$. Moreover, as the conductor of ψ divides e, we have $\psi^k(\mathfrak{a}_1^{(1)}) \equiv 1 \bmod \wp$, and $\psi^k(\mathfrak{a}_2^{(1)}) \equiv \beta^k \not\equiv 1 \bmod \wp$. Finally, both ideals are prime to S and p by construction, and $\sigma_{\mathfrak{a}_1^{(1)}} = \sigma_{\mathfrak{a}_2^{(1)}} = 1$ because the conductor of F over K also divides e. This completes the case $h = 1$.

For $h > 1$, again choose $\mathfrak{a}_1^{(h)} = (1 + ne\pi)$ and $n_2^{(h)} = -(N\mathfrak{a}_1^{(h)} - 1)$. Take $\mathfrak{a}_2^{(h)}$ to be an integral ideal of K, prime to S and p, such that $\sigma_{\mathfrak{a}_2^{(h)}} = \sigma_h^{-1}$, and let $n_1^{(h)} = N\mathfrak{a}_2^{(h)} - 1$. The proof of the lemma is now complete.

So far in this section, we have made no hypothesis on the decomposition of $\wp$ in the extension F/K, other than requiring that $\wp$ does not ramify in F/K. We now suppose, until further notice, that $\wp$ splits completely in F. We use the notation of the last part of §13. Thus $\mathscr{S}$ will denote the set of prime of $F_0 = F(E_\pi)$ above $\wp$, and $\mathscr{U}$ will again be given by (4). Let

$$i : F_0 \to \prod_{\mathfrak{q} \in \mathscr{S}} F_{0,\mathfrak{q}} \tag{15}$$

be the canonical embedding of F_0 in the product of its completions at the primes $\mathfrak{q}$ in $\mathscr{S}$. Recall that C denotes the group of elliptic units of F_0, as defined at the beginning of this section. We write $\mathfrak{C}$ for the subgroup of C consisting of all elements which are $\equiv 1 \bmod \mathfrak{q}$ for each $\mathfrak{q} \in \mathscr{S}$. Let $\overline{i(\mathfrak{C})}$ be the closure of $i(\mathfrak{C})$ in the $\wp$-adic topology. Our aim is to compute, for $1 \leq k \leq p-2$, the image of $\overline{i(\mathfrak{C})}$ under the homomorphism $\varphi_{F,k}$ given by (6).

Recall that Φ is the field $K_\wp(E_\pi)$, which lies inside our fixed algebraic closure of $K_\wp$. Since $\wp$ splits completely in F by hypothesis, the completion of F_0 at each $\mathfrak{q}$ in $\mathscr{S}$ is plainly topologically isomorphic to Φ. To simplify notation, we adopt the following convention. We fix one embedding of F_0 in Φ, and view this embedding as simply being an inclusion. This amounts to choosing one fixed prime in $\mathscr{S}$, which we denote by $\mathfrak{q}$. Let Ω denote the Galois group of F_0 over $K(E_\pi)$. Since $\wp$ is totally ramified in $K(E_\pi)$, and splits completely in $F_0/K(E_\pi)$, the other primes in $\mathscr{S}$ are given precisely by the $\mathfrak{q}^\sigma$ for $\sigma \in \Omega$, and the embedding of F_0 in Φ corresponding to $\mathfrak{q}^\sigma$ is given by σ itself. With this convention, the map (15) is simply given by

$$i(x) = (x^\sigma)_{\sigma \in \Omega}. \tag{16}$$

Now take x to be any elliptic unit in $\mathfrak{C}$. More explicitly, let $\xi(\tau)$ be the point of E_π corresponding to our chosen generator u of $\mathscr{E}_\pi$ under our fixed isomorphism from $\hat{E}$ to $\mathscr{E}$. Then, by definition, x will be of the form

$$x = \prod_{j \in J} \Lambda(\tau, \mathfrak{a}_j)^{n_j} \tag{17}$$

for some pair $(A, \mathcal{N})$ belonging to $\mathcal{I}$. Now $\Omega = G(F_0/K(E_\pi))$ is canonically isomorphic to $\mathcal{G} = G(F/K)$ under the restriction map, and we shall identify these two Galois groups in this way when there is no danger of confusion. Since Ω fixes E_π, it is then plain that

$$x^\sigma = \prod_{j\in J} \Lambda_\sigma(\tau, \mathfrak{a}_j)^{n_j} \qquad \text{for } \sigma \in \Omega,$$

where $\Lambda_\sigma(z, \mathfrak{a}_j)$ is as defined just after Lemma 7

LEMMA 14: *Let x be the elliptic unit in* $\mathfrak{C}$ *given by* (17). *Then, for each integer k with* $1 \le k \le p-2$, *we have*

$$\varphi_{F,k}(i(x)) = \left(\lambda_k \sum_{j\in J} n_j(N\mathfrak{a}_j\zeta_F(\sigma, k) - \psi^k(\mathfrak{a}_j)\zeta_F(\sigma\sigma_{\mathfrak{a}_j}, k)) \bmod \mathfrak{q}^\sigma\right)_{\sigma\in\Omega},$$

where $\lambda_k = 12(-1)^{k-1}\rho^{-k}$.

PROOF: We can obtain a power series $f_\sigma(w)$, with coefficients in $\mathcal{O}_\mathfrak{p}$, such that $f_\sigma(u) = x^\sigma$ in the following manner. Let w be the parameter of the Lubin-Tate formal group $\mathscr{E}$, and expand the rational function of $\wp(z)$ and $\wp'(z)$, with coefficients in F, given by

$$\prod_{j\in J} \Lambda_\sigma(z, \mathfrak{a}_j)^{n_j} \tag{18}$$

as a formal power series in w. Denote the power series obtained in this way by $f_\sigma(w)$. By lemma 11 and the fact that t can be written as a power series in w with coefficients in $\mathcal{O}_\mathfrak{p}$, we conclude that $f_\sigma(w)$ does indeed have coefficients in $\mathcal{O}_\mathfrak{p}$. It is then plain that $x^\sigma = f_\sigma(u)$. Moreover, as $z = w + \Sigma_{i=2}^\infty a_i w^i$, where $a_i = 0$ unless $i \equiv 1 \bmod(p-1)$ (cf. Lemma 7 of [4]), we see that the coefficients of z^k and w^k $(0 \le k \le p-1)$ in the series expansions of (18) in terms of z and w must be equal. Thus the conclusion of the lemma is now clear from Lemma 8 and the definition of $\varphi_{F,k}$.

We now come to the first main result of this section. Since the elliptic units of F_0 are stable under the action of the Galois group of F_0 over K (cf. Lemma 20 of [4]), it follows, in particular, that $\overline{i(\mathfrak{C})}$ is a $Z_p[G]$-submodule of $\mathcal{U}$, where $G = G(F_0/F)$. We can therefore take the canonical decomposition (2) of $\mathcal{U}/\overline{i(\mathfrak{C})}$. We follow the terminology of [4] and say that p is anomalous for E if $\pi + \bar{\pi} = 1$.

THEOREM 14: *Assume that p is a prime number >5 satisfying* (i) *p does not belong to the finite exceptional set S,* (ii) *p splits in K, say* $(p) = \wp\bar{\wp}$, (iii) *$\wp$ splits completely in F/K, and* (iv) *p is not anomalous for E. Let $\mathfrak{C}$ be the group of elliptic units of $F_0 = F(E_\pi)$, which are* $\equiv 1 \bmod \mathfrak{q}$ *for each* $\mathfrak{q} \in \mathcal{S}$. *Then, for each integer k with $1 \leq k \leq p-2$, the eigenspace $(\mathcal{U}/\overline{i(\mathfrak{C})})^{(k)}$ is non-trivial if and only if* $\Omega^{-kd}L_F(\bar{\psi}_F^k, k) \equiv 0 \bmod \mathfrak{q}$ *for each* $\mathfrak{q} \in \mathcal{S}$.

REMARK: By Lemma 10, $\Omega^{-kd}L_F(\bar{\psi}_F^k, k) \equiv 0 \bmod \mathfrak{q}$ for one prime $\mathfrak{q}$ in $\mathcal{S}$ if and only if the same congruence is valid for all $\mathfrak{q}$ in $\mathcal{S}$.

PROOF: We adopt the same convention as before, in which we have fixed one prime $\mathfrak{q}$ in $\mathcal{S}$, and view F_0 as being contained in Φ. We make use of the following formal identity in the group ring $F[\mathcal{G}]$, which is very reminiscent of computations with Stickelberger elements in cyclotomic fields. For each $\sigma \in \mathcal{G}$, put

$$\zeta_F^*(\sigma, k) = \lambda_k \zeta_F(\sigma, k).$$

By Corollary 9, $\zeta_F^*(\sigma, k)$ belongs to F. Write

$$\alpha = \sum_{\sigma \in \mathcal{G}} \zeta_F^*(\sigma, k)\sigma^{-1}. \tag{19}$$

Then, for each integral ideal $\mathfrak{a}$ of K which is prime to $\mathfrak{g}$, we plainly have

$$(N\mathfrak{a} - \psi^k(\mathfrak{a})\sigma_{\mathfrak{a}})\alpha = \sum_{\sigma \in \mathcal{G}} \delta_k(\sigma, \mathfrak{a})\sigma^{-1}, \tag{20}$$

where

$$\delta_k(\sigma, \mathfrak{a}) = N\mathfrak{a}\zeta_F^*(\sigma, k) - \psi^k(\mathfrak{a})\zeta_F^*(\sigma\sigma_{\mathfrak{a}}, k). \tag{21}$$

By Corollary 6, the eigenspace $(\mathcal{U}/\overline{i(\mathfrak{C})})^{(k)}$ will be trivial if and only if $\varphi_{F,k}(\overline{i(\mathfrak{C})})$ has dimension d over the finite field F_p with p elements. This suggests that we study the image under $\varphi_{F,k}$ of any d elements of $\overline{i(\mathfrak{C})}$. Suppose therefore that $(A^{(h)}, \mathcal{N}^{(h)})$ $(1 \leq h \leq d)$ are any d elements of $\mathcal{I}$. Let x_h, given by (17), be the elliptic unit corresponding to $(A^{(h)}, \mathcal{N}^{(h)})$. We assume that $x_1, \ldots, x_d$ belong to $\mathfrak{C}$. Write

$$A^{(h)} = \{\mathfrak{a}_j^{(h)} : j \in J_h\}, \quad \mathcal{N}^{(h)} = \{n_j^{(h)} : j \in J_h\},$$

and

$$\gamma_h = \sum_{j \in J_h} n_j^{(h)} (N\mathfrak{a}_j^{(h)} - \psi^k(\mathfrak{a}_j^{(h)})\sigma_{\mathfrak{a}_j^{(h)}}).$$

For $\sigma \in \mathscr{G}$ and $1 \leq h \leq d$, we define

$$b_{h\sigma} = \sum_{j \in J_h} n_j^{(h)} \delta_k(\sigma, \mathfrak{a}_j^{(h)}),$$

where $\delta_j(\sigma, \mathfrak{a}_j^{(h)})$ is given by (21). It is then plain from (20) that we have the identity

$$\gamma_h \alpha = \sum_{\sigma \in \mathscr{G}} b_{h\sigma} \sigma^{-1} \qquad (1 \leq h \leq d). \tag{22}$$

We let Ξ denote the $d \times d$-determinant form from the $b_{h\sigma}$ ($h = 1, \ldots, d$, $\sigma \in \mathscr{G}$).

By Lemma 14, the determinant of the d vectors

$$\varphi_{F,k}(i(x_h)) \qquad (1 \leq h \leq d)$$

is equal to $\Xi \bmod \mathfrak{q}$. We now proceed to compute Ξ. To this end, let $\hat{\mathscr{G}}$ be the group of homomorphisms from $\mathscr{G}$ to the multiplicative group of non-zero complex numbers. Let $\sigma_1 = 1, \sigma_2, \ldots, \sigma_d$ denote the distinct elements of $\mathscr{G}$, and $\chi_1 = 1, \chi_2, \ldots, \chi_d$ the distinct elements of $\hat{\mathscr{G}}$. Write Γ and Σ for the $d \times d$-determinants formed from the $\chi_i(\gamma_h)$, $\chi_i(\sigma_h^{-1})$ $(1 \leq i, h \leq d)$, respectively. Applying each of the χ_i to the equation (22), we conclude that

$$\left(\prod_{i=1}^{d} \chi_i(\alpha)\right)\Gamma = \Sigma\Xi. \tag{23}$$

We now make two observations. Put $L_F^*(\bar{\psi}_F^k, k) = \lambda_k^d L_F(\bar{\psi}_F^k, k)$. Then it is plain from (12) and (19) that

$$\prod_{i=1}^{d} \chi_i(\alpha) = L_F^*(\bar{\psi}_F^k, k). \tag{24}$$

Secondly, $\Sigma \neq 0$ and Γ/Σ is an algebraic integer in K. The former assertion is clear. To prove the latter one, we note that we can write

$$\gamma_h = \sum_{\sigma \in \mathscr{G}} e_{h\sigma} \sigma^{-1}, \tag{25}$$

where the $e_{h\sigma}$ are algebraic integers in K. Applying each of the χ_i to (25), it follows that $\Gamma = \Lambda\Sigma$, where Λ is the $d \times d$-determinant formed from the $e_{h\sigma}$. Since Σ is obviously an algebraic integer in K, it follows that the same is true for $\Sigma = \Gamma/\Lambda$.

We can now complete the proof of Theorem 14. Suppose first that $L_F^*(\bar{\psi}_F^k, k) \equiv 0 \bmod \mathfrak{q}$. Then we conclude from (23), (24) and the above remarks that $\Xi \equiv 0 \bmod \mathfrak{q}$ for all choices of the d pairs $(A^{(h)}, \mathcal{N}^{(h)})$ in $\mathcal{J}$. Thus $\varphi_{F,k}(\overline{i(\mathfrak{C})})$ has dimension strictly less than d over $\mathbb{F}_p$, and hence $(\mathcal{U}/i(\mathfrak{C}))^{(k)} \neq 0$. Conversely, assume that $L_F^*(\bar{\psi}_F^k, k) \neq 0 \bmod \mathfrak{q}$. Then it follows from (23) and (24) that $\Xi \not\equiv 0 \bmod \mathfrak{q}$ only if we can choose the d pairs $(A^{(h)}, \mathcal{N}^{(h)})$ such that the determinant Λ defined above is not congruent to 0 modulo $\wp$. But this is always possible. Indeed, make the choice of the d pairs $(A^{(h)}, \mathcal{N}^{(h)})$ specified in Lemma 13. Note that, by multiplying each of the $n_1^{(h)}, n_2^{(h)}$ $(1 \leq h \leq d)$ by $p-1$ (which changes none of the other conditions in Lemma 13), we can certainly assume that the corresponding elliptic units lie in $\mathfrak{C}$. Using the relation $\Sigma_{j=1}^2 n_j^{(h)}(N\mathfrak{a}_j^{(h)} - 1) = 0$ and the fact that $\psi^k(\mathfrak{a}_1^{(h)}) \equiv 1 \bmod \wp$, we conclude that

$$\gamma_h \equiv n_2^{(h)} - n_2^{(h)}\psi^k(\mathfrak{a}_2^{(h)})\sigma_h^{-1} \bmod \wp \qquad (1 \leq h \leq d);$$

here the congruence mod $\wp$ means that we have taken the coefficients in the group ring mod $\wp$. It is now trivial to verify from the other conditions of Lemma 13 that $\Lambda \not\equiv 0 \bmod \wp$. This completes the proof of Theorem 14.

Lemma 15: *There are infinitely many rational primes p satisfying conditions* (i), (ii), (iii), *and* (iv) *of Theorem* 14.

Proof: As before, let $H = K(E_g)$. Applying Cebotarev's density theorem to a Galois extension of $\mathbb{Q}$ containing H, we conclude that there are infinitely many rational primes p which split completely in H. We claim that any rational prime p, not in S, which splits completely in H, satisfies (i), (ii), (iii) and (iv). The only part which is not obvious is that such a p satisfies (iv). Take such a p, and let $(p) = \wp\bar{\wp}$ be its factorization in K. Since $\wp$ splits completely in H, the Artin symbol $(\wp, H/K)$ fixes E_g. On the other hand, as $\psi(\wp) = \pi$, Shimura's reciprocity law gives $\xi(\rho)^{(\wp, H/K)} = \xi(\pi\rho)$ for each $\rho \in E_g$. Thus we must have $\pi \equiv 1 \bmod g$. Now, if p were anomalous, it would follow that $\pi\bar{\pi} = (\pi - 1)(\bar{\pi} - 1)$, and this is clearly impossible because p was prime to g by hypothesis. This completes the proof.

We now begin the proof of the second main result of this section.

As before, let $F_n = F(E_{\pi^{n+1}})$. Since $\wp$ is totally ramified in $K(E_{\pi^{n+1}})$, it is clear that each prime of F above $\wp$ is totally ramified in F_n. Write $\mathcal{S}_n$ for the set of primes of F_n above $\wp$. Let C_n be the group of elliptic units of F_n, as defined at the beginning of this section, and let $\mathfrak{C}_n$ be the subgroup of C_n consisting of all elements which are $\equiv 1 \bmod \mathfrak{q}$ for each $\mathfrak{q} \in \mathcal{S}_n$. If $m \geq n$, we write $N_{m,n}$ for the norm map from F_m to F_n. The next lemma, which is, in essence, one of the main results of [6], is valid without any hypothesis on the decomposition of $\wp$ in F.

LEMMA 16: *For each $m \geq n \geq 0$, we have $N_{m,n}(\mathfrak{C}_m) = \mathfrak{C}_n$.*

PROOF: Recall that $\mathfrak{f}_n = \mathfrak{g}\wp^{n+1}$ is the conductor of F_n over K, by Lemma 3. Let f_n denote a generator of the ideal $\mathfrak{f}_n \cap \mathbb{Z}$, and let g_n be the largest divisor of f_n such that the g_n-th roots of unity lie in F_n. We claim that $g_n = g_0$ for all $n \geq 0$, and that g_0 is prime to p. Indeed, F_n can contain no non-trivial p-power roots of unity, because $\bar{\wp}$ does not divide the conductor of F_n/K. Moreover, since F_n/F_0 is totally ramified at the primes above $\wp$, it follows that F_n and F_0 have the same group of roots of unity for all $n \geq 0$. Let D be the group of g_0-th roots of unity in F_0. Robert (cf. [6], p. 43) has defined Ω_{F_n} to be the group DC_n. Moreover, since $\mathfrak{f}_0$ divides $\mathfrak{f}_n$ and $\mathfrak{f}_0$ and $\mathfrak{f}_n$ are divisible by the same primes, it is shown in [6] (cf. Proposition 17, p. 43) that $N_{m,n}(\Omega_{F_m})D = \Omega_{F_n}$. Since the order of D is prime to p (and hence no element of D is $\equiv 1 \bmod \mathfrak{q}$ for $\mathfrak{q} \in \mathcal{S}_n$), it follows immediately that $N_{m,n}(\mathfrak{C}_m) = \mathfrak{C}_n$. This completes the proof.

For each integer $n \geq 0$, let $\Phi_n = K_\wp(E_{\pi^{n+1}})$, and let $\wp_n$ be the maximal ideal of Φ_n. Write U_n for the units of Φ_n which are $\equiv 1 \bmod \wp_n$, and U'_n for the subgroup of U_n consisting of all elements with norm 1 to $K_\wp$. Plainly

$$(U'_n)^{(k)} = U_n^{(k)} \qquad \text{for} \qquad k \not\equiv 0 \bmod (p-1). \tag{26}$$

If $m > n$, we also write $N_{m,n}$ for the norm map from Φ_m to Φ_n.

LEMMA 17: *Suppose that $k \not\equiv 0 \bmod (p-1)$. If $m \geq n$, then the norm map from $U_m^{(k)}$ to $U_n^{(k)}$ is surjective, and its kernel is equal to $(U_m^{(k)})^{1-\tau}$, where τ is a generator of $G(\Phi_m/\Phi_n)$.*

PROOF: The norm map from U'_m to U'_n is surjective, because U'_n consists of those elements of U_n which are norms from Φ_m for all $m \geq n$ (cf. Lemma 8 of [4]). Thus the first assertion is plain from (26). As for the second, let V_m denote the kernel of the norm map from U_m

to U_n. Since Φ_m/Φ_n is a totally ramified cyclic extension of degree p^{m-n}, a standard computation (cf. [5], p. 188) shows that

$$[V_m : U_m^{1-\tau}] = [V_m^{(0)} : U_m^{(0)(1-\tau)}] = p^{m-n}.$$

Hence $[V_m^{(k)} : U_m^{(k)(1-\tau)}] = 1$ for all $k \not\equiv 0 \bmod (p-1)$, as required.

The following elementary lemma is certainly well known, but we have been unable to find a suitable reference.

LEMMA 18: *Let Λ be a cyclic group of prime order $p \neq 2$, operating on a finitely generated $\mathbb{Z}_p$-module M. Let τ be a generator of Λ. If $M = (\tau - 1)M$, then $M = 0$.*

PROOF: Since $\tau^p = 1$ and p is odd, it is clear that

$$(\tau - 1)^p \in p\mathbb{Z}[\Lambda], \tag{27}$$

where $\mathbb{Z}[\Lambda]$ is the group ring of Λ with coefficients in $\mathbb{Z}$. Let N be the torsion submodule of M, so that M/N is a free $\mathbb{Z}_p$-module of finite rank with $(\tau-1)(M/N) = (M/N)$. But this shows that $(\tau-1)^p$ is surjective on M/N, and this is impossible by (27) unless $M/N = 0$. Hence we can suppose that M is a finite abelian p-group. But again (27) implies that $M = 0$ if $(\tau - 1)M = M$. This completes the proof.

For each $\mathfrak{q} \in \mathcal{S}_n$, let $F_{n,\mathfrak{q}}$ be the completion of F_n at $\mathfrak{q}$, and again let i be the canonical inclusion of F_n in $\Pi_{\mathfrak{q}\in\mathcal{S}_n} F_{n,\mathfrak{q}}$. Write $U_{n,\mathfrak{q}}$ for the units in $F_{n,\mathfrak{q}}$ which are $\equiv 1 \bmod \mathfrak{q}$, and put

$$\mathcal{U}_n = \prod_{\mathfrak{q}\in\mathcal{S}_n} U_{n,\mathfrak{q}}. \tag{28}$$

Thus, in terms of our earlier notation, $\mathcal{U}_0 = \mathcal{U}$ and $\mathfrak{E}_0 = \mathfrak{E}$.

THEOREM 19: *Let p be a prime number satisfying* (i) *p does not belong to S,* (ii) *p splits in K, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, and* (iii) *$\mathfrak{p}$ splits completely in F. Let k be an integer with $1 \le k \le p-2$. Let m, n be any two integers ≥ 0, with $m > n$. Then $(\mathcal{U}_m/\overline{i(\mathfrak{E}_m)})^{(k)} \neq 0$ if and only if $(\mathcal{U}_n/\overline{i(\mathfrak{E}_n)})^{(k)} \neq 0$.*

PROOF: Since $\mathfrak{p}$ splits completely in F, we can identify $F_{n,\mathfrak{q}}$, for each $\mathfrak{q} \in \mathcal{S}_n$, with the field Φ_n, and $U_{n,\mathfrak{q}}$ with U_n. Let $N_{m,n} : \mathcal{U}_m \to \mathcal{U}_n$ be the map given by the product of the local norms from Φ_m to Φ_n at each $\mathfrak{q} \in \mathcal{S}_n$. Suppose now that $1 \le k \le p-2$. Put $A_n = \mathcal{U}_n^{(k)}/\overline{i(\mathfrak{E}_n)}^{(k)}$. It follows from the first part of Lemma 17 that the norm map from $\mathcal{U}_m^{(k)}$ to $\mathcal{U}_n^{(k)}$ is surjective, whence the induced map from $A_m^{(k)}$ to $A_n^{(k)}$ is also surjective. Thus it is clear that $A_m^{(k)} = 0$ implies that $A_n^{(k)} = 0$. To prove the converse, we note that Lemmas 16 and 17 together imply that the kernel of the norm map from $A_m^{(k)}$ to $A_n^{(k)}$ is $(A_m^{(k)})^{1-\tau}$, where τ is a generator of the Galois group of F_m over F_n. Suppose now that $A_n^{(k)} = 0$. Since $A_{n+1}^{(k)}$ is a finitely generated $\mathbf{Z}_p$-module, we conclude from Lemma 18 that $A_{n+1}^{(k)} = 0$. Repeating the argument a finite number of times, it follows that $A_m^{(k)} = 0$ for all $m \geq n$. This completes the proof.

5. Proof of Theorem 1

We can now complete the proof of Theorem 1 in an entirely similar fashion to the proof of Theorem 1 in [4]. If N is an abelian extension of F_n, which is Galois over F, then $G_n = G(F_n/F)$ operates on $X = G(N/F_n)$ via inner automorphisms in the usual way. In particular, $G = G(F_0/F)$ operates on X, because we can identify G with a subgroup of G_n. Thus, if N is a p-extension of F_n, we can take the canonical decomposition (2) of X into eigenspaces for the action of G.

As before, let $\mathcal{S}_n$ be the set of primes of F_n over $\wp$. Let M_n denote the maximal abelian p-extension of F_n, which is unramified outside $\mathcal{S}_n$, and let L_n be the p-Hilbert class field of F_n. Let $\mathcal{U}_n$ be defined by (28), that is, $\mathcal{U}_n$ is the product of the local units $\equiv 1$ in the completions of F_n at the primes $\mathfrak{q} \in \mathcal{S}_n$. Write $N_{F_n/K}: \mathcal{U}_n \to K_\wp$ for the map given by the product of the local norms at all $\mathfrak{q} \in \mathcal{S}_n$. We denote the kernel of $N_{F_n/K}$ by $\mathcal{U}'_n$. Plainly

$$\text{(29)} \qquad \mathcal{U}_n^{(k)} = (\mathcal{U}'_n)^{(k)} \qquad \text{whenever} \qquad k \not\equiv 0 \bmod (p-1).$$

As is explained in detail in [3], global class field theory gives the following explicit description of $G(M_n/L_nF_\infty)$ as a G_n-module, where $F_\infty = \bigcup_{n\geq 0} F_n$. Let E_n be the group of all global units of F_n which are $\equiv 1 \bmod \mathfrak{q}$ for each $\mathfrak{q} \in \mathcal{S}_n$. Let $\overline{i(E_n)}$ be the closure of $i(E_n)$ in $\mathcal{U}_n$ in the $\wp$-adic topology.

THEOREM 20: *For each $n \geq 0$, $\mathcal{U}'_n/\overline{i(E_n)}$ is isomorphic as a G_n-module, via the Artin map, to $G(M_n/L_nF_\infty)$.*

Suppose now that there does exist a point P in $E(F)$ of infinite order. Take p to be a rational prime satisfying (i) p does not belong to S, (ii) p splits in K, $(p) = \wp\bar{\wp}$, and (iii) $\wp$ splits completely in F. As before, let $\pi = \psi(\wp)$. For each $n \geq 0$, choose Q_n in $E(\bar{F})$ such that $\pi^{n+1}Q_n = P$, and form the extension $H_n = F_n(Q_n)$. Thus H_n/F_n is a cyclic extension of degree dividing p^{n+1}, and as P lies in $E(F)$, one verifies easily that

$$(30) \qquad x^\sigma = \chi(\sigma)x \qquad \text{for all } x \in G(H_n/F_n) \quad \text{and} \quad \sigma \in G.$$

An entirely similar argument to that given in Lemma 33 of [4] shows that H_n/F_n is unramified outside $\mathcal{S}_n$. Finally, as $\wp$ splits completely in F, the local arguments in Theorem 11 and Lemma 35 of [4] again show that the extension H_nF_∞/F_∞ is non-trivial and ramified for all sufficiently large n.

Assume now that n is so large that H_nF_∞/F_∞ is non-trivial and ramified. Hence the extension $H_nL_nF_\infty/L_nF_\infty$ is non-trivial. As this extension lies inside M_n, we conclude from (29), (30) and Theorem 20 that

$$(31) \qquad (\mathcal{U}_n/\overline{i(E_n)})^{(1)} \neq 0.$$

As before, let $\mathfrak{C}_n$ be the group of elliptic units of F_n, which are $\equiv 1 \bmod \mathfrak{q}$ for each $\mathfrak{q} \in \mathcal{S}_n$. As $\mathfrak{C}_n \subset E_n$, it follows that $(\mathcal{U}_n/\overline{i(\mathfrak{C}_n)})^{(1)} \neq 0$. Therefore, by Theorem 19, $(\mathcal{U}_0/\overline{i(\mathfrak{C}_0)})^{(1)} \neq 0$. Assume, in addition, that $p > 5$ and is not anomalous for E. Theorem 14 then implies that

$$\Omega^{-d}L_F(\bar{\psi}_F, 1) \equiv 0 \bmod \mathfrak{q} \qquad \text{for each } \mathfrak{q} \in \mathcal{S}_n.$$

But, by Lemma 15, there certainly are infinitely many rational primes p satisfying the conditions we have imposed on p. Thus $\Omega^{-d}L_F(\bar{\psi}_F, 1)$ is divisible by infinitely many distinct prime ideals of F, and so must be equal to 0. Since the Hasse-Weil zeta function of E over F is equal to $L_F(\psi_F, s)L_F(\bar{\psi}_F, s)$, up to finitely many Euler factors which do not vanish at $s = 1$ (cf. Theorem 7.42 of [7]), this completes the proof of Theorem 1.

REFERENCES

[1] N. ARTHAUD: On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication II (in preparation).
[2] J. COATES: p-Adic L-functions and Iwasawa's theory (to appear in Proceedings of Durham symposium on algebraic number theory).
[3] J. COATES, A. WILES: Kummer's criterion for Hurwitz numbers (to appear in

Proceedings of International Conference on algebraic number theory, Kyoto, Japan, 1976).

[4] J. COATES, A. WILES: On the conjecture of Birch and Swinnerton-Dyer (to appear in Inventiones Mathematicae).

[5] S. LANG: *Algebraic Number Theory*, Addison-Wesley, 1970.

[6] G. ROBERT: Unités elliptiques. *Bull. Soc. Math. France, Mémoire 36*, 1973.

[7] G. SHIMURA: Introduction to the arithmetic theory of automorphic functions. *Pub. Math. Soc. Japan, 11*, 1971.

(Oblatum 27-I-1977)

Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
16 Mill Lane
Cambridge, England