J. Austral. Math. Soc. (*Series A*) **26** (1978), 1–25

ON p-ADIC L-FUNCTIONS AND ELLIPTIC UNITS

J. COATES and A. WILES

Dedicated to Kurt Mahler on his 75th birthday

(Received 2 December 1977)

Communicated by J. B. Miller

Abstract

The aim of the paper is to prove an elliptic analogue of a deep theorem of Iwasawa on cyclotomic fields.

Subject classification (*Amer. Math. Soc.* (*MOS*) *1970*): primary 12 A 35, 12 A 65.

Introduction

Let $\zeta(s)$ denote the Riemann zeta function. Euler showed that $(2\pi\sqrt{-1})^{-k}\,\zeta(k)$ is rational for each even integer $k>0$. Subsequently, Kummer discovered two remarkable connections between these special values of $\zeta(s)$ and the arithmetic of cyclotomic fields. The best known of these is Kummer's criterion for the irregularity of a prime number p. The second, which we now describe, has received less attention. Let $\mathbf{Q}$ be the rational field, p an odd prime number, and μ_p the group of p-th roots of unity. Let $F_0=\mathbf{Q}(\mu_p)$, and write G_0 for the Galois group of F_0 over $\mathbf{Q}$. We denote by χ the canonical character, with values in the p-adic integers $\mathbf{Z}_p$, giving the action of G_0 on μ_p. There is a unique prime $\mathfrak{p}_0$ of F_0 above p, and we write U_0 for the local units of the completion of F_0 at $\mathfrak{p}_0$, which are $\equiv 1 \bmod \mathfrak{p}_0$. Let C_0 be the group of classical cyclotomic units of F_0 which are $\equiv 1 \bmod \mathfrak{p}_0$, and $\bar{C}_0$ the closure of C_0 in U_0 in the $\mathfrak{p}_0$-adic topology. For each integer i modulo $(p-1)$, we write $(U_0/\bar{C}_0)^{(i)}$ for the eigenspace of $U_0/\bar{C}_0$ on which G_0 acts via χ^i. Kummer proved that, for each even integer k with $1<k<p-1$, the eigenspace $(U_0/\bar{C}_0)^{(k)}$ is

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

non-zero if and only if $(2\pi\sqrt{-1})^{-k}\zeta(k)\equiv 0 \bmod p$. In two important papers, Iwasawa (1964, 1969) established a deep generalization of Kummer's theorem. Let F_∞ be the field obtained by adjoining all p-power roots of unity to $\mathbf{Q}$, and let F be any finite extension of $\mathbf{Q}$ contained in F_∞. Then Iwasawa's work gave an explicit description as modules over the group ring $\mathbf{Z}_p[G(F/\mathbf{Q})]$, of the analogous quotient for F of local units modulo the closure of the cyclotomic units, in terms of the p-adic L-functions of Kubota–Leopoldt.

In our previous paper (Coates–Wiles, 1977), we established an elliptic analogue of Kummer's theorem (see Theorem 29 of that paper), and used it to prove part of the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication. It is natural to ask whether there is also an elliptic analogue of Iwasawa's generalization of Kummer's theorem. The aim of the present paper is to show that this is, in fact, the case. Our method of proof is quite different from that given by Iwasawa, and can be used to give a substantially simpler proof in the cyclotomic case (for an account of our method in the cyclotomic case, see Lang (to appear)). Let K be an imaginary quadratic field with class number 1, and $\mathcal{O}$ the ring of integers of K. Let E be an elliptic curve defined over K, with complex multiplication by $\mathcal{O}$, and let ψ be the Grossencharacter of E over K. Throughout this paper, S will denote the set consisting of 2, 3 and all rational primes q such that E has a bad reduction at at least one prime of K above q. Choose p to be a rational prime, which is not in the finite exceptional set S, and which splits in K, say $(p) = \mathfrak{p}\bar{\mathfrak{p}}$. We fix one of the factors $\mathfrak{p}$ of p in K. Put $\pi = \psi(\mathfrak{p})$, so that π is a generator of $\mathfrak{p}$. Now, as E has complex multiplication by $\mathcal{O}$, we can also view π as an endomorphism of E. For each $n\geqslant 0$, let $E_{\pi^{n+1}}$ be the kernel of the endomorphism π^{n+1} of E, and let $F_n = K(E_{\pi^{n+1}})$. Then $\mathfrak{p}$ is totally ramified in F_n, and we write $\mathfrak{p}_n$ for the unique prime of F_n lying above $\mathfrak{p}$. Let U_n be the local units of the completion of F_n at $\mathfrak{p}_n$, which are $\equiv 1 \bmod \mathfrak{p}_n$. Let C_n be Robert's group of elliptic units for the field F_n (for the precise definition, see Section 3), and $\bar{C}_n$ the closure of C_n in U_n in the $\mathfrak{p}_n$-adic topology. Write G_0 for the Galois group of F_0 over K. Denote by χ the canonical character, with values in $\mathbf{Z}_p$, giving the action of G_0 on E_π. For each integer i modulo $(p-1)$, we write $(U_n/\bar{C}_n)^{(i)}$ for the eigenspace of $U_n/\bar{C}_n$ on which G_0 acts via χ^i. We henceforth assume that $i\not\equiv 0$ modulo $(p-1)$, because the case $i\equiv 0$ modulo $(p-1)$ is both less interesting and requires a slightly different treatment. Let $F_\infty = \bigcup_{n\geqslant 0} F_n$, and write Γ for the Galois group of F_∞ over F_0. Our aim is to determine the structure of

$$Y_\infty^{(i)} = \varprojlim (U_n/\bar{C}_n)^{(i)},$$

where the projective limit is taken relative to the norm maps, as a module over Γ. Let $\Lambda = \mathbf{Z}_p[[T]]$ be the ring of formal power series in an indeterminate T with coefficients in $\mathbf{Z}_p$. Fix a topological generator γ_0 of Γ. Then the Γ-module structure

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

on $Y_\infty^{(i)}$ gives rise to a unique Λ-module structure satisfying $(1+T)y = \gamma_0 y$ for all y in $Y_\infty^{(i)}$. Now it is not very difficult to show that $Y_\infty^{(i)}$ is pseudo-isomorphic as a Λ-module to some quotient module of Λ. However, much deeper arguments are required to determine explicitly which quotient actually occurs. The remarkable fact, first discovered by Iwasawa in the cyclotomic case, is that the answer involves p-adic L-functions. Fix a Weierstrass model for E

$$(1) \qquad y^2 = 4x^3 - g_2 x - g_3$$

such that g_2, g_3 belong to $\mathcal{O}$, and the discriminant of (1) is divisible only by primes of K lying above primes in S. Let L be the period lattice of the Weierstrass $\mathfrak{p}$-function associated with this model. Since K has class number 1, there exists $\Omega \in L$ such that $L = \Omega\mathcal{O}$. For each integer $k \geqslant 1$, let $L(\bar\psi^k, s)$ be the complex Hecke L-function of $\bar\psi^k$, where $\bar\psi^k$ is viewed as a (not necessarily primitive) Grossencharacter modulo the conductor of $\bar\psi$. It has been shown by Hurwitz, Birch and Swinnerton-Dyer, and Damerell that the numbers $\Omega^{-k} L(\bar\psi^k, k)$ $(k = 1, 2, \ldots)$ belong to K. We can therefore view these numbers as lying not only in the complex field, but also in the completion $K_\mathfrak{p}$ of K at the non-archimedean prime $\mathfrak{p}$. Let $\Omega_\mathfrak{p}$ denote the completion of the maximal unramified extension of $K_\mathfrak{p}$, and $\mathscr{I}_\mathfrak{p}$ the ring of integers of $\Omega_\mathfrak{p}$. For each non-zero residue class i modulo $(p-1)$, we prove the existence of a power series $G_i(T)$ in $\mathscr{I}_\mathfrak{p}[[T]]$, with the following interpolation property (see Theorem 18). Let κ be the canonical character giving the action of Γ on $E_{\pi^{n+1}}$ $(n = 0, 1, \ldots)$, and put $u = \kappa(\gamma_0)$. Write $\mathfrak{f}$ for the conductor of ψ, and let $f \in K$ be a fixed generator of $\mathfrak{f}$. For each integer $k \geqslant 1$, write

$$(2) \qquad \mu_k = 12(-1)^{k-1}(k-1)!\,(\Omega/f)^{-k}.$$

Then

$$(3) \qquad G_i(u^k - 1) = \gamma^{1-k}\mu_k\left(1 - \frac{\psi(\mathfrak{p})^k}{N\mathfrak{p}}\right) L(\bar\psi^k, k)$$

for all integers $k > 0$ with $k \equiv i$ modulo $(p-1)$; here γ is a certain unit in $\mathscr{I}_\mathfrak{p}$, which should be viewed intuitively as the $\mathfrak{p}$-adic analogue of the period Ω of E. In fact, the existence of such power series $G_i(T)$ is already contained in earlier work of Katz (1977), Lichtenbaum (to appear) and Manin-Vishik (1974). The novelty of the present paper is to relate $G_i(T)$ to the Iwasawa module $Y_\infty^{(i)}$. We say that p is anomalous for E if $\pi + \bar\pi \equiv 1 \bmod p$, where $\pi = \psi(\mathfrak{p})$ (see Lemma 12 of Coates-Wiles (1977)). For each $n \geqslant 0$, write $\omega_n (1+T)^{p^n} - 1$.

THEOREM 1. *Assume that* (i) *p does not belong to S,* (ii) *p splits in K, say $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, and* (iii) *$p$ is not anomalous for E. Then, for each non-zero residue class i modulo $(p-1)$, $Y_\infty^{(i)}$ is isomorphic as a Λ-module to $\Lambda/(\mathscr{G}_i(T))$, where $\mathscr{G}_i(T)$ is a power series in Λ, which generates the same ideal in $\mathscr{I}_\mathfrak{p}[[T]]$ as the power series $G_i(T)$ satisfying* (3). *Moreover, $Y_\infty^{(i)}/\omega_n Y_\infty^{(i)}$ is Λ-isomorphic to $(U_n/\bar{C}_n)^{(i)}$ for all $n \geqslant 0$.*

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

As is crucial in the proof of the main result of Coates–Wiles (1977), there are always infinitely many primes p satisfying conditions (i), (ii) and (iii) of Theorem 1. However, it should be noted that Theorem 1 remains valid if we remove condition (iii) on the prime p, provided we only insist that $Y_{\infty}^{(1)}$ be pseudo-isomorphic to $\Lambda/(\mathscr{G}_1(T))$, but still require that $Y_{\infty}^{(i)}$ be Λ-isomorphic to $Y_{\infty}^{(i)}$ for all $i \not\equiv 0, 1$ modulo $(p-1)$. We hope to give a detailed proof of this in a subsequent paper.

Finally, we mention an unsolved problem, which was one of our main motivations in proving Theorem 1. Let M_∞ be the maximal abelian p-extension of F_∞, which is unramified outside the unique prime of F_∞ above $\mathfrak{p}$. Write X_∞ for the Galois group of M_∞ over F_∞, and G_∞ for the Galois group of F_∞ over K. Then $G_\infty = G_0 \times \Gamma$ operates on X_∞ in the natural way, via inner automorphisms. If we write $\mathrm{X}_{\infty}^{(i)}$ for the eigenspace of X_∞ on which G_0 acts via χ^i, then $\mathrm{X}_{\infty}^{(i)}$ is a compact Γ-module, and hence also a Λ-module. Let i be a non-zero residue class modulo $(p-1)$. Is it true that $\mathrm{X}_{\infty}^{(i)}$ has the same characteristic power series as $Y_{\infty}^{(i)}$? A positive answer to this question in the case $i \equiv 1$ modulo $(p-1)$ would, in view of Theorem 1, have deep consequences for the study of the arithmetic of the elliptic curve E. We see no way of settling this problem at present. Also the cyclotomic analogue (see the Main Conjecture in Coates (1977)) is still unsolved.

1. Notation

We mainly use the notation of our earlier paper (Coates–Wiles, 1977). In particular, 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. We let E be an elliptic curve defined over K, whose endomorphism ring is isomorphic to $\mathcal{O}$. The finite set S of rational primes is defined as in the Introduction, and we fix a Weierstrass model (1) for E such that g_2, g_3 belong to $\mathcal{O}$, and the discriminant of (1) is prime to S. Let $\mathfrak{p}(z)$ be the Weierstrass function associated with (1), and L the period lattice of $\mathfrak{p}(z)$. Put $\xi(z) = (\mathfrak{p}(z), \mathfrak{p}'(z))$. As usual, we identify $\mathcal{O}$ with the endomorphism ring of E in such a way that the endomorphism corresponding to α in $\mathcal{O}$ is given by $\xi(z) \mapsto \xi(\alpha z)$. Let ψ be the Grossencharacter of E over K in the sense defined in Shimura (1971), Section 7.8. As before, we write $\mathfrak{f}$ for the conductor of ψ. We denote by Ω an element of the period lattice L such that $L = \Omega\mathcal{O}$.

We fix, for the rest of the paper, a rational prime p satisfying conditions (i), (ii) and (iii) of Theorem 1. Put $\pi = \psi(\mathfrak{p})$. For each $n \geqslant 0$, let $E_{\pi^{n+1}}$ be the kernel of the endomorphism π^{n+1} of E, and let $F_n = K(E_{\pi^{n+1}})$. Then $\mathfrak{p}$ is totally ramified in F_n, and we write $\mathfrak{p}_n$ for the unique prime of F_n lying above $\mathfrak{p}$. Let Φ_n be the completion of F_n at $\mathfrak{p}_n$. Our assumption that p is not anomalous for E is equivalent to the assertion that Φ_n contains no nontrivial p-th root of unity for all integers $n \geqslant 0$ (cf. Lemma 12 of Coates–Wiles (1977)). Let U_n be the group of units of Φ_n,

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

which are $\equiv 1 \bmod \mathfrak{p}_n$. Of course, U_n is a $\mathbf{Z}_p$-module in the natural way. Put

$$\Phi_\infty = \bigcup_{n\geqslant 0} \Phi_n, \quad F_\infty = \bigcup_{n\geqslant 0} F_n$$

Write G_∞ for the Galois group of F_∞ over K or, equivalently, the Galois group of Φ_∞ over $K_\mathfrak{p}$. Let $E_\infty = \bigcup_{n\geq 0} E_{\pi^{n+1}}$, and let κ: $G_\infty \to \mathbf{Z}_p^\times$ be the character giving the action of G_∞ on E_∞, i.e. $u^\sigma = \kappa(\sigma)u$ for all $\sigma \in G_\infty$ and $u \in E_\infty$. Plainly $G_\infty = \Gamma \times G_0$, where $\Gamma = G(F_\infty/F_0)$, and where G_0 is cyclic of order $p-1$ and can be identified with the Galois group of F_0 over K. Let χ denote the restriction of κ to G_0, so that χ generates $\operatorname{Hom}(G_0, \mathbf{Z}_p^\times)$. If A is any $\mathbf{Z}_p[G_0]$-module, we define $A^{(i)}$ to be the submodule of A on which G_0 acts via χ^i. Thus we have the canonical decomposition

$$A = \bigoplus_{i=1}^{p-1} A^{(i)}.$$

Let Λ be the ring of formal power series in an indeterminate T, with coefficients in $\mathbf{Z}_p$. Let B be a compact $\mathbf{Z}_p$-module, on which Γ operates continuously. Fix a topological generator γ_0 of Γ. Then, as usual, B has a unique Λ-module structure such that $\gamma_0 x = (1+T)x$ for all x in B. If B and C are Λ-modules, we say that B is pseudo-isomorphic to C if there exists a Λ-homomorphism from B to C with finite kernel and cokernel. For each $n \geqslant 0$, write $\omega_n = (1+T)^{p^n} - 1$.

Let $\hat{E}$ be the formal group giving the kernel of reduction modulo $\mathfrak{p}$ on E. The parameter of $\hat{E}$ is

$$t = -2x/y = -2\wp(z)/\wp'(z). \tag{4}$$

We can view z as being the parameter of the formal additive group G_a, and then (4) is the exponential map of $\hat{E}$. Let $\mathcal{O}_\mathfrak{p}$ be the ring of integers of $K_\mathfrak{p}$ (of course, we can identify $\mathcal{O}_\mathfrak{p}$ with $\mathbf{Z}_p$). We write E for the unique formal group defined over $\mathcal{O}_\mathfrak{p}$ such that the endomorphism $[\pi]$ of E is given by $[\pi](w) = \pi w + w^p$. By Lubin–Tate theory, there is a unique isomorphism from $\hat{E}$ to E over $\mathcal{O}_\mathfrak{p}$, of the form

$$w = t + \sum_{k=2}^{\infty} h_k t^k. \tag{5}$$

We write

$$\lambda\colon \mathrm{E} \xrightarrow{\sim} G_a \quad \text{and} \quad \varphi\colon G_a \xrightarrow{\sim} \mathrm{E} \tag{6}$$

for the logarithm and exponential maps, respectively, of E. Of course, the map $w = \varphi(z)$ is just the composition of (4) and (5). Finally, E_{π^n} will denote the kernel of the endomorphism $[\pi^n]$ of E.

2. The local theory

We remind the reader that we are assuming throughout that p is not anomalous for E, or equivalently that the field Φ_∞ contains no non-trivial p-power roots of unity. The principal result of this section is Theorem 5, which is the key to the whole paper. It is curious that it seems to have been overlooked prior to this. In fact, Theorem 5 remains true both when p is anomalous for E, and also for the eigenspace given by $i \equiv 0$ modulo $(p-1)$, but the proof is more difficult in these cases, and we have omitted it. The theorem has been considerably generalized by R. Coleman (to appear), who has also given a more conceptual method of proof.

Let Φ_n^{x} be the multiplicative group of non-zero elements of Φ_n. For each $m \geqslant n$, we write $N_{m,n}$ for the norm map from Φ_m to Φ_n, and we put

$$\Phi_n' = \bigcap_{m \geqslant n} N_{m,n}(\Phi_m^{x}).$$

It is easy to see (cf. Lemma 8 of Coates–Wiles (1977)) that Φ_n' is the subgroup of Φ_n^{x} consisting of all elements whose norm to $K_{\mathfrak{p}}$ is a power of $\pi = \psi(\mathfrak{p})$. For each $n \geqslant 0$, we define

$$X_n = \varprojlim \Phi_n'/\Phi_n'^{p},$$

the projective limit being taken relative to the obvious maps. If $m \geqslant n$, the norm map from Φ_m to Φ_n clearly gives rise to a map from X_m to X_n ,which we also denote by $N_{m,n}$. Let $X_\infty = \varprojlim X_n$, where the projective limit is taken relative to the $N_{m,n}$. We endow X_∞ with its natural structure as a G_∞-module. In particular, X_∞ is a compact Γ-module, and thus also a Λ-module. Recall that

$$\omega_n = (1+T)^{p^n} - 1.$$

Recall also that U_n denotes the units of Φ_n, which are $\equiv 1 \bmod \mathfrak{p}_n$.

LEMMA 2. (i) *For all $i \not\equiv 0$ modulo $(p-1)$, we have*

$$X_n^{(i)} = U_n^{(i)}, \quad X_\infty^{(i)} = \varinjlim U_n^{(i)},$$

where the projective limit on the right is taken relative to the norm maps.

(ii) *For all i modulo $(p-1)$, and all integers $n \geqslant 0$, we have $X_\infty^{(i)}/\omega_n X_\infty^{(i)}$ is isomorphic as a Λ-module to $X_n^{(i)}$.*

PROOF. It is easy to see (cf. formula (47) of Coates–Wiles (1977)) that we have an exact sequence of G_∞-modules

$$0 \to U_n' \to X_n \to \mathbf{Z}_p \to 0,$$

where U_n' denotes the elements in U_n with norm 1 to $K_{\mathfrak{p}}$; here G_∞ operates trivially on $\mathbf{Z}_p$. Hence

$$X_n^{(i)} = U_n'^{(i)} = U_n^{(i)}$$

for all $i \not\equiv 0$ modulo $(p-1)$. This is the first assertion of (i), and the second assertion follows immediately. Assertion (ii) follows from the interpretation of X_∞ and X_n as Galois groups, via the local Artin map. Indeed, let M_∞ be the maximal abelian p-extension of Φ_∞, and M_n the maximal abelian p-extension of Φ_n. Since $M_\infty/K_{\mathfrak{p}}$ is a Galois extension, G_∞ operates on the abelian normal subgroup $G(M_\infty/\Phi_\infty)$ of $G(M_\infty/K_{\mathfrak{p}})$ in the natural way, via inner automorphisms (cf. Coates (1977)). By local class field theory, the local Artin map defines a G_∞-isomorphism from X_n to $G(M_n/\Phi_n)$ for all $n \geqslant 0$, and consequently a G_∞-isomorphism from X_∞ to $G(M_\infty/\Phi_\infty)$ on passing to the projective limit. Now it is plain that M_n is the maximal abelian extension of Φ_n contained in M_∞. From this, it follows easily (cf. Coates (1977)) that we must have $X_\infty/\omega_n X_\infty = X_n$ for all $n \geqslant 0$. This completes the proof of the lemma.

COROLLARY 3. *Assume that* $i \not\equiv 0$ *modulo* $(p-1)$. *Then* $X_\infty^{(i)}$ *is a free* Λ*-module of rank* 1.

PROOF. Since p is not anomalous for E, U_n has no torsion for all $n \geqslant 0$, and so $U_n^{(i)}$ is a free $\mathbf{Z}_p$-module of finite rank for all i modulo $(p-1)$. Let $\mathcal{O}_n$ be the ring of integers of Φ_n, G_n the Galois group of Φ_n over $K_{\mathfrak{p}}$, and log the p-adic logarithm. Now there is a submodule V_n of finite index in U_n such that log V_n is contained in $\mathcal{O}_n$ as a submodule of finite index. On the other hand, it is clear that $\mathcal{O}_n$ contains as a submodule of finite index a free module of rank 1 over the group ring $\mathbf{Z}_p[G_n]$. These two remarks clearly imply that $U_n^{(i)}$ is a free $\mathbf{Z}_p$-module of rank p^n for all i modulo $(p-1)$.

By Lemma 2, $X_\infty^{(i)}/\omega_n X_\infty^{(i)}$ is isomorphic to $U_n^{(i)}$, where we now assume that $i \not\equiv 0$ modulo $(p-1)$. It follows from the structure theory of finitely generated Λ-modules that $X_\infty^{(i)}$ must be pseudo-isomorphic to Λ. But $X_\infty^{(i)} = \varprojlim U_n^{(i)}$ has no $\mathbf{Z}_p$-torsion, because each $U_n^{(i)}$ has no torsion. Hence there is an exact sequence of Λ-modules

$$0 \to X_\infty^{(i)} \to \Lambda \to D \to 0,$$

where D is a finite Λ-module. Let $\Gamma_n = G(\Phi_\infty/\Phi_n)$. Since D is finite, we have $D^{\Gamma_n} = D$ for all sufficiently large n. However, the snake lemma implies that D^{Γ_n} injects into $X_\infty^{(i)}/\omega_n X_\infty^{(i)} = U_n^{(i)}$ for all $n \geqslant 0$. Hence D must be 0 because $U_n^{(i)}$ has no torsion. This completes the proof of the corollary.

We now explicitly construct a basis for $X_\infty^{(i)}$ over Λ, for all $i \not\equiv 0$ modulo $(p-1)$. Write e_i for the orthogonal idempotent of χ^i in $\mathbf{Z}_p[G_0]$, i.e.

$$e_i = (p-1)^{-1} \sum_{\sigma \in G_0} \chi^{-i}(\sigma)\,\sigma.$$

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

We now fix, for the rest of the paper, a vector (u_n) $(n = 0, 1, \ldots)$ such that (i) each u_n is a generator of $\mathrm{E}_{\pi^{n+1}}$, and (ii) $N_{m,n}(u_m) = u_n$ for all $m \geqslant n$. In other words, (u_n) is a basis of the Tate module $T_\pi = \varprojlim \mathrm{E}_{\pi^{n+1}}$ as a module over $\mathbf{Z}_p$.

THEOREM 4. *Let β denote the unique $(p-1)$-th root of $1-\pi$ satisfying $\beta \equiv 1 \bmod p$. Then we have $N_{m,n}(\beta - u_m) = \beta - u_n$ for all $m \geqslant n$. Moreover, for $i \not\equiv 0$ modulo $(p-1)$, the element $((\beta - u_n)^{e_i})$ $(n = 0, 1, \ldots)$ is a basis of $X_\infty^{(i)}$ over Λ.*

PROOF. To prove the first assertion, it suffices to show that $N_{n,n-1}(\beta - u_n) = \beta - u_{n-1}$ for all $n \geqslant 1$. Since the minimal equation for u_n over Φ_{n-1} is $X^p + \pi X - u_{n-1} = 0$, it follows that the minimal equation for $\beta - u_n$ is

$$(\beta - X)^p + \pi(\beta - X) - u_{n-1} = 0.$$

Thus $N_{n,n-1}(\beta - u_n) = \beta^p + \pi\beta - u_{n-1}$, and this last quantity is equal to $\beta - u_{n-1}$, because $\beta^p + (\pi - 1)\beta = 0$ (by the definition of β).

Suppose now that $1 \leqslant i < p-1$. Now $(\beta - u_n)^{e_i}$ belongs to $U_n^{(i)}$ for all $n \geqslant 0$. We claim that $(\beta - u_0)^{e_i}$ generates $U_0^{(i)}$ as a $\mathbf{Z}_p$-module. Indeed, as $U_0^{(i)}$ is a free $\mathbf{Z}_p$-module of rank 1, it suffices to show that the image of $(\beta - u_0)^{e_i}$ in $U_0^{(i)}/U_0^{(i)p}$ is non-zero. As is explained in Section 4 of Coates–Wiles (1977) (cf. Lemmas 9 and 10), this latter assertion is true if and only if

$$\varphi_i((\beta - u_0)^{e_i}) = \varphi_i(\beta - u_0) \not\equiv 0 \mod p,$$

where φ_i is the homomorphism defined in Section 4 of Coates–Wiles (1977). We can compute $\varphi_i(\beta - u_0)$ as follows. A suitable power series for $\beta - u_0$ is $f(w) = \beta - w$ (note that we do not have to assume that $f(w)$ has constant term 1 because $i < p-1$). Hence

$$w\frac{d}{dw}\log f(w) = -\sum_{k=1}^{\infty} (w/\beta)^k,$$

and so $\varphi_i(\beta - u_0) \equiv -\beta^{-i} \not\equiv 0 \bmod p$, as required.

Let α be the element of $X_\infty^{(i)}$ given by $\alpha = ((\beta - u_n)^{e_i})$, and put $Y_\infty^{(i)} = \Lambda\alpha$. Now $X_\infty^{(i)}$ and $Y_\infty^{(i)}$ are compact Γ-modules. Hence, to show that $Y_\infty^{(i)} = X_\infty^{(i)}$, it suffices to verify that $Z_\infty^{(i)}/TZ_\infty^{(i)} = 0$, where $Z_\infty^{(i)} = X_\infty^{(i)}/Y_\infty^{(i)}$. This is equivalent to showing that the canonical map g from $Y_\infty^{(i)}/TY_\infty^{(i)}$ to $X_\infty^{(i)}/TX_\infty^{(i)}$ is surjective. But, by Lemma 2, the projection of $X_\infty^{(i)}$ onto its 0-th factor induces an isomorphism from $X_\infty^{(i)}/TX_\infty^{(i)}$ to $U_0^{(i)}$. The projection of $Y_\infty^{(i)}$ to its 0-th factor thus induces a homomorphism from $Y_\infty^{(i)}/TY_\infty^{(i)}$ to $U_0^{(i)}$, and by the result of the previous paragraph this homomorphism is surjective. Hence g is surjective, and this completes the proof of Theorem 4.

THEOREM 5. *Assume that $i \not\equiv 0$ modulo $(p-1)$. For each $\alpha = (\alpha_n)$ belonging to $X_\infty^{(i)} = \varprojlim U_n^{(i)}$, there exists a unique power series $f_\alpha(T)$ in Λ such that $f_\alpha(u_n) = \alpha_n$ for all $n \geqslant 0$.*

PROOF. The uniqueness is obvious from the Weierstrass preparation theorem. As for the existence, we note first that the element $\alpha = ((\beta - u_n)^{e_i})$ $(n = 0, 1, \ldots)$ of Theorem 4 satisfies the assertion of Theorem 5. Indeed, recalling Lemma 6 of Coates–Wiles (1977), we can plainly take

$$f_\alpha(w) = \prod_{\sigma \in G_0} (\beta - \chi(\sigma)\, w)^{\chi^{-i}(\sigma)/(p-1)}.$$

Secondly, we observe that the set B of all elements α of $X_\infty^{(i)}$ satisfying the assertion of Theorem 5 is a Λ-submodule. Indeed, B is clearly a $\mathbf{Z}_p$-submodule. It is also a Λ-submodule because, if $\alpha \in B$ and $\sigma \in \Gamma$, the power series associated with $\alpha^\sigma = (\alpha_n^\sigma)$ is $f_\alpha \circ [\kappa(\sigma)]$. Thus Theorem 5 is plain from Theorem 4.

3. Elliptic units

In this section, we establish a number of basic results about the elliptic units of Robert (1973), which will subsequently play a central role in the proof of Theorem 1.

If $\mathscr{L}$ is any lattice in the complex plane, let

$$\sigma(z, \mathscr{L}) = z \prod_{\substack{\omega \in \mathscr{L} \\ \omega \neq 0}} (1 - z/\omega) \exp\left(\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)$$

be the Weierstrass σ-function of $\mathscr{L}$. Let

$$\theta(z, \mathscr{L}) = \Delta(\mathscr{L}) \exp(-6 s_2(\mathscr{L})\, z^2)\, \sigma(z, \mathscr{L})^{12},$$

where $\Delta(\mathscr{L})$ is the discriminant function of $\mathscr{L}$, and $s_2(\mathscr{L})$ is as defined at the beginning of Section 5 of Coates–Wiles (1977).

Recall that $L = \Omega\mathcal{O}$ is the period lattice of our elliptic curve (1). If $\mathfrak{a}$ is an arbitrary integral ideal of K, we define

$$\Theta(z, \mathfrak{a}) = \theta(z, L)^{N\mathfrak{a}} / \theta(z, \mathfrak{a}^{-1} L),$$

where $N\mathfrak{a}$ is the absolute norm of $\mathfrak{a}$, and $\mathfrak{a}^{-1} L$ denotes the lattice $\Omega\mathfrak{a}^{-1}$. In fact, it is not difficult to see that $\Theta(z, \mathfrak{a})$ is an elliptic function for the lattice L (for an explicit expression for $\Theta(z, \mathfrak{a})$ as a rational function of $\wp(z)$, see formula (23) of Coates–Wiles (1977)).

We now establish a basic property of the function $\Theta(z, \mathfrak{a})$. First, we introduce some notation, which will be used repeatedly throughout the rest of the paper. Let $\mathfrak{g}$ be an arbitrary integral ideal of K. We define $\mathscr{S}_\mathfrak{g}$ to be the set consisting of

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

all pairs

$$\mathfrak{s} = (A, \mathscr{N}), \tag{7}$$

where $A = \{\mathfrak{a}_j : j \in J\}$ and $\mathscr{N} = \{n_j : j \in J\}$; here J is an arbitrary finite index set, the $\mathfrak{a}_j$ are integral ideals of K prime to $6\mathfrak{g}$, and the n_j are rational integers satisfying

$$\sum_{j \in J} n_j(N\mathfrak{a}_j - 1) = 0. \tag{8}$$

Given any such pair $\mathfrak{s} = (A, \mathscr{N})$ in $\mathscr{S}_{\mathfrak{g}}$, we define

$$\Theta(z, \mathfrak{s}) = \prod_{j \in J} \Theta(z, \mathfrak{a}_j)^{n_j}, \tag{9}$$

and, for each integer $k \geqslant 0$, we put

$$h_k(\mathfrak{s}) = \sum_{j \in J} n_j(N\mathfrak{a}_j - \psi^k(\mathfrak{a}_j)). \tag{10}$$

We shall only use the symbol $\mathfrak{s}$ to denote elements of $\mathscr{S}_{\mathfrak{g}}$, so that there will be no danger of confusion between the function $\Theta(z, \mathfrak{s})$ defined by (9) and the function $\Theta(z, \mathfrak{a})$ defined in the preceding paragraph for an integral ideal $\mathfrak{a}$ of K.

LEMMA 6. *Let g be any generator of the ideal $\mathfrak{g}$. Then, for each $\mathfrak{s}$ in $\mathscr{S}_{\mathfrak{g}}$, we have*

$$\prod_{\eta} \Theta(z + \eta, \mathfrak{s}) = \Theta(gz, \mathfrak{s}), \tag{11}$$

where the product on the left is taken over a set $\{\eta\}$ of representatives modulo L of the $\mathfrak{g}$-division points of L.

PROOF. It follows from the definition of $\Theta(z, \mathfrak{a}_j)$ that the zeros of $\Theta(z, \mathfrak{a}_j)$ occur precisely at the elements of L, each with multiplicity $12(N\mathfrak{a}_j - 1)$. Similarly, the poles of $\Theta(z, \mathfrak{a}_j)$ are each of order 12, and occur precisely at the elements of $\mathfrak{a}_j^{-1}L$, which are not in L. Using this remark, one sees easily that the functions on the right- and left-hand sides of (11) have the same zeros and poles, counted with multiplicity. Since both sides are elliptic functions, it follows that the ratio of the right- and left-hand sides of (11) must be a constant C. To evaluate C, we let $z \to 0$ on both sides of (11). Let γ_j be a generator of the ideal $\mathfrak{a}_j$. Now $\Theta(z, \mathfrak{a}_j)/z^{12(N\mathfrak{a}_j - 1)}$ tends to $\Delta(L)^{N\mathfrak{a}_j}/\Delta(\mathfrak{a}_j^{-1}L) = \Delta(L)^{N\mathfrak{a}_j - 1}\gamma_j^{-12}$ as $z \to 0$. In view of (8), it follows that the right-hand side of (11) tends to $\prod_{j \in J} \gamma_j^{-12n_j}$ as $z \to 0$. Similarly, the left-hand side of (11) tends to $\varepsilon \prod_{j \in J} \gamma_j^{-12n_j}$, where $\varepsilon = \prod_{\eta \neq 0} \Theta(\eta, \mathfrak{s})$, the product being taken over all non-zero η modulo L. For any non-zero $\mathfrak{g}$-division point η of L, Robert (1973) has shown that $\Theta(\eta, \mathfrak{s})$ is a unit in the ray class field H of K modulo $\mathfrak{g}$. Moreover, in view of (8), it follows from Proposition 9 of Robert (1973) that $\Theta(\eta, \mathfrak{s})$ is the 12-th power of an element of H. Further, if $\mathfrak{b} = (b)$ is an integral ideal of K prime to $\mathfrak{g}$, it is easy to see either from Proposition 9 of Robert (1973)

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

or from formula (27) of Coates–Wiles (1977) that

$$\Theta(\eta, \mathfrak{s})^{\sigma_{\mathfrak{b}}} = \Theta(b\eta, \mathfrak{s}),$$

where $\sigma_{\mathfrak{b}}$ is the Artin symbol of $\mathfrak{b}$ for H/K. It follows easily that

$$\varepsilon = (N_{H/K}\,\Theta(\eta, \mathfrak{s}))^r,$$

where $N_{H/K}$ denotes the norm from H to K, and r is an integer $\geqslant 1$. As $\Theta(\eta, \mathfrak{s})$ is a 12-th power in H, and the group of units of K has exponent 12, we conclude that $\varepsilon = 1$. This completes the proof of the lemma.

We now return to our elliptic curve E given by equation (1). Recall that $\mathfrak{f}$ denotes the conductor of the Grossencharacter ψ of E. Fix a generator f in K of the ideal $\mathfrak{f}$, and put $\rho = \Omega/f$. Thus $\xi(\rho) = (\mathfrak{p}(\rho), \mathfrak{p}'(\rho))$ is a generator as an $\mathcal{O}$-module of the group $E_{\mathfrak{f}}$ of f-division points of E. Let B denote an arbitrary set of representatives, which are integral and prime to $\mathfrak{f}$, of the ray class group of K modulo $\mathfrak{f}$. If $\mathfrak{a}$ is an arbitrary integral ideal of K prime to $6\mathfrak{f}$, we define

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

LEMMA 7. $\Lambda(z, \mathfrak{a})$ *does not depend on the choice of the set B of representatives of the ray class group of K modulo $\mathfrak{f}$.*

PROOF. Let $\mathfrak{b}$, $\mathfrak{c}$ be integral ideals of K, prime to $\mathfrak{f}$, which belong to the same ray class modulo $\mathfrak{f}$, i.e. $\mathfrak{b} = (\gamma)\,\mathfrak{c}$, where $\gamma \equiv 1 \bmod^* \mathfrak{f}$. Then, as $\mathfrak{f}$ is the conductor of ψ, we have $\psi(\mathfrak{b}) = \gamma\psi(\mathfrak{c})$. Thus $\psi(\mathfrak{b}) - \psi(\mathfrak{c}) = (\gamma - 1)\,\psi(\mathfrak{c})$ is an integer in K, which is divisible by $\mathfrak{f}$. Consequently, $\psi(\mathfrak{b})\,\rho$ and $\psi(\mathfrak{c})\,\rho$ differ by an element of the period lattice L, whence the assertion of the lemma is plain.

From now on, we write $\mathscr{S}$ for the index set $\mathscr{S}_{\mathfrak{f}\mathfrak{p}}$, consisting of all pairs $\mathfrak{s} = (A, \mathscr{N})$, where $A = \{\mathfrak{a}_j : j \in J\}$ and $\mathscr{N} = \{n_j : j \in J\}$; here J is an arbitrary finite index set, the $\mathfrak{a}_j$ are integral ideals of K prime to $6\mathfrak{f}\mathfrak{p}$, and the n_j are rational integers satisfying (8). Note that in our 1977 paper we insisted that the ideals $\mathfrak{a}_j$ had to be prime to both S and p. However, it is easy to see that all the arguments of that paper remain valid if we require only that the $\mathfrak{a}_j$ be prime to $6\mathfrak{f}\mathfrak{p}$, as in the present paper. For each pair $\mathfrak{s} = (A, \mathscr{N})$ in $\mathscr{S}$, we define

$$\Lambda(z, \mathfrak{s}) = \prod_{j \in J} \Lambda(z, \mathfrak{a}_j)^{n_j}.$$

LEMMA 8. *Let $\pi = \psi(\mathfrak{p})$. Then, for each integer $n \geqslant 0$, we have*

$$\prod_{\eta} \Lambda(z + \eta, \mathfrak{s}) = \Lambda(\pi^n z, \mathfrak{s}),$$

where the product on the left is taken over a set $\{\eta\}$ of representatives modulo L of the π^n-division points of L.

PROOF. Since π^n is a generator of the ideal $\mathfrak{p}^n$, it follows from Lemma 6 that

$$\prod_{\eta} \Theta(z+\eta+\psi(\mathfrak{b})\rho, \mathfrak{s}) = \Theta(\pi^n z+\psi(\mathfrak{p}^n\mathfrak{b})\rho, \mathfrak{s}).$$

But, as $\mathfrak{b}$ runs over a set of representatives, integral and prime to $\mathfrak{f}$, of the ray class group modulo $\mathfrak{f}$, so does $\mathfrak{p}^n\mathfrak{b}$. Thus Lemma 8 is plain from Lemma 7.

Recall that in Section 2, we fixed a generator u_n of $\mathrm{E}_{\pi^{n+1}}$ for all $n\geqslant 0$, with the property that $[\pi^{m-n}](u_m)=u_n$ for all $m\geqslant n$. Now choose τ_n modulo L such that $-2\mathfrak{p}(\tau_n)/\mathfrak{p}'(\tau_n)$ is the image in $\hat{E}_{\pi^{n+1}}$ of u_n under the isomorphism (5) from $\hat{E}$ to E. When there is no danger of confusion, we briefly express the relation between u_n and τ_n as $u_n=\varphi(\tau_n)$, where φ is the exponential map of E. Plainly, we have $\pi^{m-n}\tau_m\equiv\tau_n \bmod L$ for all $m\geqslant n$.

It is shown in Coates–Wiles (1977) that $\Lambda(z,\mathfrak{s})$ is a rational function of $\mathfrak{p}(z)$ and $\mathfrak{p}'(z)$ with coefficients in K, for each $\mathfrak{s}\in\mathscr{S}$. Moreover, as is explained in detail in that paper the numbers $\Lambda(\tau_n,\mathfrak{s})$, for $\mathfrak{s}$ ranging over $\mathscr{S}$, form a subgroup C_n of the group of global units of $F_n=K(E_{\pi^{n+1}})$. We recall that, as explained above, $\mathscr{S}$ is now a slightly larger index set than that used in Coates–Wiles (1977), but the arguments remain the same. These units were first defined by Robert (1973) and will be called the elliptic units of F_n. It is not difficult to verify (see Lemma 20 of our paper) that C_n is independent of the choice of the primitive π^{n+1}-division point τ_n of L, and is stable under the action of the Galois of F_n over K. If $m\geqslant n$, we write $N_{m,n}$ for the norm map from F_m to F_n.

LEMMA 9. *For each $\mathfrak{s}$ in $\mathscr{S}$, and each $m\geqslant n$, we have*

$$N_{m,n}(\Lambda(\tau_m,\mathfrak{s}))=\Lambda(\tau_n,\mathfrak{s}).$$

In particular, the map $N_{m,n}\colon C_m\to C_n$ is surjective.

PROOF. For each $n\geqslant 0$, let $\mathscr{R}_n$ be the ray class field of K modulo $\mathfrak{f}_n=\mathfrak{f}\mathfrak{p}^{n+1}$. By Lemma 4 of Coates–Wiles (1977), we have $\mathscr{R}_n=K(E_{\mathfrak{f}\pi^{n+1}})$, where $E_{\mathfrak{f}\pi^{n+1}}$ denotes the group of $\mathfrak{f}\pi^{n+1}$-division points of E. Now fix integers $m\geqslant n\geqslant 0$. Take $\mathfrak{c}$ to be any integral ideal of K, prime to $\mathfrak{f}\mathfrak{p}$, whose Artin symbol $\sigma_{\mathfrak{c}}=(\mathfrak{c},\mathscr{R}_m/K)$ fixes the subfield $\mathscr{R}_n$ of $\mathscr{R}_m$. Then we claim that

$$\Lambda(\tau_m,\mathfrak{s})^{\sigma_{\mathfrak{c}}}=\Lambda(\tau_m+\delta_{\mathfrak{c}},\mathfrak{s}), \tag{12}$$

where $\delta_{\mathfrak{c}}$ is a π^{m-n}-division point of L (which depends on $\mathfrak{c}$). Suppose this is true for the moment. Since we can identify the Galois group of $\mathscr{R}_m/\mathscr{R}_n$ with the Galois group of F_m/F_n, and since $\pi^{m-n}\tau_m\equiv\tau_n \bmod L$, it follows that every conjugate of

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

$\Lambda(\tau_m, \mathfrak{s})$ over F_n is given by $\Lambda(\nu, \mathfrak{s})$, where ν is some π^{m-n}-division point modulo L of τ_n. But, as $[F_m : F_n] = p^{m-n}$, the number of conjugates of $\Lambda(\tau_m, \mathfrak{s})$ over F_n is equal to the number of π^{m-n}-division points modulo L of τ_n. Hence we must have

$$N_{m,n}(\Lambda(\tau_m, \mathfrak{s})) = \prod_{\nu} \Lambda(\nu, \mathfrak{s}), \tag{13}$$

where ν runs over a set of representatives modulo L of the π^{m-n}-division points of τ_n. But, by Lemma 8, the right-hand side of (13) is equal to $\Lambda(\tau_n, \mathfrak{s})$, and so (13) is just the assertion of Lemma 9.

To complete the proof, we must establish (12). By hypothesis, the Artin symbol $\sigma_{\mathfrak{c}}$ fixes $\mathscr{R}_n = K(E_{\mathfrak{f}\pi^{n+1}})$. Now, by the definition of ψ, we have $\xi(\alpha)^{\sigma_{\mathfrak{c}}} = \xi(\psi(\mathfrak{c})\,\alpha)$ for all α in $E_{\mathfrak{f}\pi^{n+1}}$. Hence we must have

$$\psi(\mathfrak{c}) \equiv 1 \mod \mathfrak{f}\mathfrak{p}^{n+1}. \tag{14}$$

In particular, for each $\mathfrak{b} \in B$, we conclude from (14) that (cf. formula (27) of Coates–Wiles (1977))

$$\Theta(\tau_m + \psi(\mathfrak{b})\,\rho, \mathfrak{s})^{\sigma_{\mathfrak{c}}} = \Theta(\psi(\mathfrak{c})\,\tau_m + \psi(\mathfrak{b})\,\rho, \mathfrak{s}).$$

Taking the product over all $\mathfrak{b}$ in B, and noting that (14) implies that

$$\pi^{m-n}(\psi(\mathfrak{c})\,\tau_m - \tau_m) \equiv 0 \mod L,$$

(12) follows, as required. This completes the proof of Lemma 9.

We can interpret Lemma 9 as asserting that, for each $\mathfrak{s}$ in $\mathscr{S}$, the vector $(\Lambda(\tau_n, \mathfrak{s}))$ $(n = 0, 1, \ldots)$ belongs to $\varprojlim U_n$, where the projective limit is taken relative to the norm maps. More importantly, if e_i is the orthogonal idempotent of χ^i in $\mathbf{Z}_p[G_0]$, we also know the unique power series in $\Lambda = \mathbf{Z}_p[[w]]$ (often we shall take w instead of T to be the variable in the ring Λ of formal power series with coefficients in $\mathbf{Z}_p$), which is attached to $(\Lambda(\tau_n, \mathfrak{s})^{e_i})$ by Theorem 5. Indeed, define the power series $R(w, \mathfrak{s})$ by

$$R(w, \mathfrak{s}) = \Lambda(\lambda(\omega), \mathfrak{s}), \tag{15}$$

where λ is the logarithm map of the formal group E. By Lemma 24 of Coates–Wiles (1977), $R(w, \mathfrak{s})$ has coefficients in $\mathbf{Z}_p$ and constant term equal to 1. Moreover, as $\Lambda(z, \mathfrak{s})$ is a rational function of $\mathfrak{p}(z)$ and $\mathfrak{p}'(z)$ with coefficients in K, it is plain that

$$R(u_n, \mathfrak{s}) = \Lambda(\tau_n, \mathfrak{s}) \tag{16}$$

for all $n \geqslant 0$. Since the formal group E has the property that $[\chi(\sigma)](w) = \chi(\sigma)\,w$ for all σ in G_0 (see Lemma 6 of our paper), we have therefore proven the following theorem.

THEOREM 10. *For each i modulo $(p-1)$, and each $\mathfrak{s}$ in $\mathscr{S}$, define the power series $R(w,\mathfrak{s})^{(i)}$ by*

$$R(w,\mathfrak{s})^{(i)} = \prod_{\sigma\in G_0} R(\chi(\sigma)\,w,\mathfrak{s})^{\chi^{-i}(\sigma)/(p-1)}.$$

Then $R(w,\mathfrak{s})^{(i)}$ has coefficients in $\mathbf{Z}_p$, and satisfies

$$R(u_n,\mathfrak{s})^{(i)} = \Lambda(\tau_n,\mathfrak{s})^{e_i} \quad \textit{for all } n \geqslant 0.$$

Finally, we give a slightly modified form of Lemma 21 of our paper, which is of fundamental importance in the proof of Theorem 1.

THEOREM 11. *For each i modulo $(p-1)$, and each $\mathfrak{s}$ in $\mathscr{S}$, we have*

$$(17)\qquad \frac{d}{dz}\log R(\varphi(z),\mathfrak{s})^{(i)} = \sum_{\substack{k=1\\ k\equiv i \bmod (p-1)}}^{\infty} c_k(\mathfrak{s})\,z^{k-1},$$

where

$$c_k(\mathfrak{s}) = 12(-1)^{k-1}\rho^{-k}h_k(\mathfrak{s})L(\bar{\psi}^k,k) \quad (k=1,2,\ldots),$$

and $h_k(\mathfrak{s})$ is given by (10).

PROOF. By the chain rule, the left-hand side of (17) is given by

$$(p-1)^{-1}\sum_{\sigma\in G_0}\chi^{1-i}(\sigma)\frac{d}{d\xi}\log\Lambda(\xi,\mathfrak{s}),$$

where $\xi = \chi(\sigma)z$. The assertion of the theorem is now plain from Lemma 21 of Coates and Wiles (1977).

4. p-adic logarithmic derivatives

A central role in the proof of Theorem 29 of Coates–Wiles (1977) is given by a type of p-adic logarithmic derivative (cf. the maps φ_i defined on p. 230). This notion seems to have its origin in Kummer's work on cyclotomic fields. The purpose of this section is to give a refinement of this notion, which is of vital importance for the proof of Theorem 1. This refinement was first suggested to us by the explicit reciprocity law given in Wiles (1978).

Recall that κ denotes the canonical character giving the action of $G_\infty = G(\Phi_\infty/K_\mathfrak{p})$ on $E_\infty = \bigcup_{n=0}^{\infty} E_{\pi^{n+1}}$. Let A and B be two G_∞-modules, which are also $\mathbf{Z}_p$-modules. If j is an integer $\geqslant 0$, we say that a $\mathbf{Z}_p$-homomorphism $g\colon A\to B$ is a κ^j-homomorphism if $g(a^\tau) = \kappa^j(\tau)g(a)^\tau$ for all $a\in A$ and $\tau\in G_\infty$. Suppose now that A is a compact G_∞-module, and so, in particular, a compact Γ-module. As usual, A has a unique Λ-module structure satisfying $\gamma_0 x = (1+T)x$ for all x in A; here γ_0 is our fixed topological generator of Γ. Put $u = \kappa(\gamma_0)$. Suppose now that $B = \mathbf{Z}_p$, with the trivial action of G_∞. Then, if g is any κ^j-homomorphism from A to B,

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

we claim that

$$g(h(T)\,\alpha) = h(u^j - 1)\,g(\alpha) \tag{18}$$

for all α in A and $h(T)$ in Λ. Indeed, this is plain when $h(T) = T$, and it follows in general by linearity and continuity.

Recall that w denotes the parameter of the formal group E, and z the parameter of the formal additive group G_a. These parameters are related by

$$z = \lambda(w), \quad w = \varphi(z), \tag{19}$$

where λ and φ are the logarithm and exponential maps of E, respectively. As before, we shall often use w instead of T as the variable in the ring $\Lambda = \mathbf{Z}_p[[T]]$. By a basic property of the logarithm map of formal groups, the derivative $\lambda'(w)$ of $\lambda(w)$ both belongs to Λ, and is a unit in Λ. Hence

$$\frac{d}{dz}f(w) = f'(w)/(\lambda'(w))$$

belongs to Λ for each $f(w)$ in Λ, and

$$\frac{d}{dz}\log f(w) = f'(w)/(f(w)\,\lambda'(w))$$

belongs to Λ for each unit $f(w)$ in Λ. Let k be an integer $\geqslant 1$. Combining the two previous remarks, we conclude that, for each unit $f(w)$ in Λ, the value

$$\left(\frac{d}{dz}\right)^k \log f(w)\bigg|_{z=0}$$

belongs to $\mathbf{Z}_p$.

For the rest of this section, i will denote an arbitrary non-zero residue class modulo $(p-1)$. As in Section 2, we write $X_\infty^{(i)} = \varprojlim U_n^{(i)}$. Let $\alpha = (\alpha_n)$ be an arbitrary element of $X_\infty^{(i)}$. By Theorem 5, there is a unique power series $f_\alpha(w)$ in Λ such that $f_\alpha(u_n) = \alpha_n$ for all $n \geqslant 0$. For each integer $k \geqslant 1$, we define the map

$$\delta_k \colon X_\infty^{(i)} \to \mathbf{Z}_p$$

by

$$\delta_k(\alpha) = \left(\frac{d}{dz}\right)^k \log f_\alpha(\varphi(z))\bigg|_{z=0}.$$

Note that $\delta_k(\alpha)$ belongs to $\mathbf{Z}_p$ by the remarks made in the previous paragraph, because $f_\alpha(w)$ is plainly a unit in Λ. It is clear also that δ_k is a $\mathbf{Z}_p$-homomorphism. If $\sigma \in G_\infty$, the power series for $\alpha^\sigma = (\alpha_n^\sigma)$ is $f_\alpha \circ [\kappa(\sigma)]$. Since

$$[\kappa(\sigma)] \circ \varphi(z) = \varphi(\kappa(\sigma)\,z),$$

it follows that δ_k is a κ^k-homomorphism from $X_\infty^{(i)}$ to $\mathbf{Z}_p$. In particular, we conclude that $\delta_k(\alpha) = 0$ unless $k \equiv i$ modulo $(p-1)$.

There is a second natural κ^k-homomorphism

$$D_k\colon X_\infty^{(i)} \to \mathbf{Z}_p,$$

which occurs in our work. If $\alpha = (\alpha_n)$ is an arbitrary element of $X_\infty^{(i)}$, we write, as above, $f_\alpha(w)$ for the power series in Λ such that $f_\alpha(u_n) = \alpha_n$ for all $n \geqslant 0$. Let T_0 denote the trace map from Φ_0 to $\mathbf{Q}_p$. For each integer $k \geqslant 1$, we define

$$D_k(\alpha) = T_0\left\{\left(\frac{d}{dz}\right)^k \log f_\alpha(\varphi(z))\Big|_{\varphi(z)=u_0}\right\}.$$

Again it is easy to see that $D_k(\alpha)$ belongs to $\mathbf{Z}_p$, and that D_k is a κ^k-homomorphism from $X_\infty^{(i)}$ to $\mathbf{Z}_p$. As $X_\infty^{(i)}$ is a free Λ-module of rank 1, it is plain that a $\mathbf{Z}_p$-multiple of δ_k must be equal to a $\mathbf{Z}_p$-multiple of D_k. The following more precise result is true.

LEMMA 12. *For each integer $k \geqslant 1$ with $k \equiv i$ modulo $(p-1)$, we have $D_k = (\pi^k - 1)\,\delta_k$, where $\pi = \psi(\mathfrak{p})$.*

PROOF. It plainly suffices to show that

$$D_k(\alpha) = (\pi^k - 1)\,\delta_k(\alpha) \tag{20}$$

for some α in $X_\infty^{(i)}$ such that $D_k(\alpha)$ and $\delta_k(\alpha)$ are both non-zero. Curiously, it does not seem easy to prove this without appealing to the elliptic units†. Suppose first that $\mathfrak{s} = (A, \mathcal{N})$ is an arbitrary element of $\mathcal{S}$. Take $\alpha = (\alpha_n)$, where $\alpha_n = \Lambda(\tau_n, \mathfrak{s})^{e_i}$ $(n = 0, 1, \ldots)$. By Theorem 10, the corresponding power series is $f_\alpha(w) = R(w, \mathfrak{s})^{(i)}$, whence we conclude from Theorem 11 that

$$\delta_k(\alpha) = \mu_k h_k(\mathfrak{s}) L(\bar{\psi}^k, k), \tag{21}$$

where μ_k is given by (2). Next we compute $D_k(\alpha)$. Let M be a set of representatives modulo L of the non-zero π-division points of L. One sees easily that

$$D_k(\alpha) = \sum_{\eta \in M} \left(\frac{d}{dz}\right)^k \log R(\varphi(z), \mathfrak{s})^{(i)}\Big|_{z=\eta}.$$

Appealing to the definition of $R(w, \mathfrak{s})^{(i)}$, we conclude that

$$D_k(\alpha) = (p-1)^{-1} \sum_{\sigma \in G_0} \chi^{k-i}(\sigma) \sum_{\eta \in M} \left(\frac{d}{d\xi}\right)^k \log \Lambda(\xi, \mathfrak{s})\Big|_{\xi = \chi(\sigma)\eta}.$$

As η ranges over M, it is clear that $\chi(\sigma)\eta$ also ranges over a set of representatives modulo L of the non-zero π-division points of L. Recalling that $k \equiv i$ modulo

† R. Coleman has pointed out to us a simple local proof of Lemma 12.

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

$(p-1)$, it follows that

$$D_k(\alpha) = \sum_{\eta \in M} \left(\frac{d}{d\xi}\right)^k \log \Lambda(\xi+\eta, \mathfrak{s})\Big|_{\xi=0}.$$

But, by Lemma 8, we have

$$\sum_{\eta \in M} \left(\frac{d}{d\xi}\right)^k \log \Lambda(\xi+\eta, \mathfrak{s}) = \left(\frac{d}{d\xi}\right)^k (\log(\Lambda(\pi\xi, \mathfrak{s})/\Lambda(\xi, \mathfrak{s}))).$$

It is now plain from Theorem 11 that

$$D_k(\alpha) = \mu_k(\pi^k - 1)\, h_k(\mathfrak{s})\, L(\bar{\psi}^k, k). \tag{22}$$

The formulae (21) and (22) are valid for all $\mathfrak{s}$ in $\mathscr{S}$, and for all integers $k \geqslant 1$ with $k \equiv i$ modulo $(p-1)$. The argument now breaks up into cases. Suppose first that $k \geqslant 3$. Under this assumption, $L(\bar{\psi}^k, k)$ is given by the convergent infinite product

$$L(\bar{\psi}^k, k) = \prod_{(\mathfrak{y}, \mathfrak{f})=1} (1 - \bar{\psi}^k(\mathfrak{y})/(N\mathfrak{y})^k)^{-1},$$

and hence is non-zero. Also, we can choose $\mathfrak{s}$ in $\mathscr{S}$ such that $h_k(\mathfrak{s}) \neq 0$ (cf. Lemma 28 of Coates–Wiles (1977), where it is shown that we can even choose $\mathfrak{s}$ in $\mathscr{S}$ such that $h_k(\mathfrak{s}) \not\equiv 0 \bmod \mathfrak{p}$, because i is not the zero residue class modulo $(p-1)$). Thus $\delta_k(\alpha)$ and $D_k(\alpha)$ are both non-zero, and (20) is valid for this choice of α. To handle the cases $k = 1$ and $k = 2$, we must use the elements of $X_\infty^{(i)}$, which are constructed in Theorem 4. We first make some general remarks about these elements, which are valid for all non-zero residue classes i modulo $(p-1)$. Let β be the unique $(p-1)$-th root of $1-\pi$ satisfying $\beta \equiv 1 \bmod p$. Let $\alpha = (\alpha_n)$, where $\alpha_n = (\beta - u_n)^{e_i}$. By Theorem 4, α belongs to $X_\infty^{(i)}$, and, as remarked in the proof of Theorem 5, the power series corresponding to α is plainly

$$f_\alpha(w) = \prod_{\alpha \in G_0} (\beta - \chi(\sigma)\, w)^{\chi^{-i}(\sigma)/(p-1)}.$$

Hence

$$\log f_\alpha(w) = \left(-\beta^{-1} \sum_{\substack{k=0 \\ k \equiv i-1 \bmod (p-1)}}^{\infty} w^k/\beta^k\right) . 1/(\lambda'(w)). \tag{23}$$

Without loss of generality, we can suppose that i is an integer satisfying $1 \leqslant i < p-1$. We claim that, for this choice of α, we have

$$\delta_i(\alpha) = -(i-1)!\, \beta^{-i} \quad (1 \leqslant i < p-1). \tag{24}$$

To prove this, we recall that the formal group E has the property that $[\zeta](w) = \zeta w$ for all $(p-1)$-th roots of unity ζ (cf. Lemma 6 of Coates–Wiles (1977)). Thus the power series $w = \varphi(z)$ must satisfy $\varphi(\zeta z) = \zeta\varphi(z)$ for all $(p-1)$-th roots of unity ζ, whence $\varphi(z)$ must be of the form $\varphi(z) = z + \sum_{n=2}^{\infty} a_n z^n$, where $a_n = 0$ unless

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

$n \equiv 1 \bmod (p-1)$. It follows easily that

$$\frac{d}{dz}\log f_\alpha(w) = -z^{i-1}/\beta^i + z^{p-1}g(z),$$

where $g(z)$ is some power series in $K_p[[z]]$. Thus (24) is plain from this last equation. By contrast, we see no easy way of computing $D_i(\alpha)$ for all i with $1 \leqslant i < p-1$. Fortunately, to prove Lemma 12, we need only calculate $D_1(\alpha)$ and $D_2(\alpha)$, and we now proceed to do this by a tedious direct calculation. If we differentiate both sides of the equation

$$\lambda([\pi](w)) = \pi\lambda(w)$$

with respect to w, it follows that

$$\pi\lambda'(w) = (\pi + pw^{p-1})\lambda'([\pi](w)).$$

Differentiating again with respect to w, we obtain

$$\pi\lambda''(w) = (\pi + pw^{p-1})^2\lambda''([\pi](w)) + p(p-1)w^{p-2}\lambda'([\pi](w)).$$

Substituting $w = u_0$ into these last two equations, and recalling that

$$u_0^{p-1} = -\pi, \quad \lambda'(0) = 1, \quad \lambda''(0) = 0,$$

we conclude that

(25) $$\lambda'(u_0) = 1-p, \quad \lambda''(u_0) = -p(p-1)u_0^{-1}.$$

From the first of these equations and (23), we obtain

$$D_1(\alpha) = \beta^{-1}(p-1)^{-1}T_0\Biggl(\sum_{\substack{k=0\\ k\equiv 0 \bmod (p-1)}}^{\infty} u_0^k/\beta^k\Biggr).$$

Using the facts $u_0^{p-1} = -\pi$ and $\beta^{p-1} = 1-\pi$, it follows easily that, in this case, $D_1(\alpha) = -(\pi-1)\beta^{-1}$. Hence (20) holds for $k = 1$ and this choice of α. Finally, consider the case $k = 2$. Differentiating both sides of (23) with respect to z, we obtain

$$\left(\frac{d}{dz}\right)^2 \log f_\alpha(w) = B(w) + C(w),$$

where

$$B(w) = \Biggl(-\beta^{-1}\sum_{\substack{k=0\\ k\equiv 1 \bmod (p-1)}}^{\infty} kw^{k-1}/\beta^k\Biggr).1/(\lambda'(w))^2$$

and

$$C(w) = \Biggl(\beta^{-1}\sum_{\substack{k=0\\ k\equiv 1 \bmod (p-1)}}^{\infty} w^k/\beta^k\Biggr)\lambda''(w)/(\lambda'(w))^3.$$

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

Using equations (25) and again the fact that $\beta^{p-1} = 1-\pi$, we conclude easily that

$$T_0(B(u_0)) = (1-\pi)\beta^{-2}(\pi-(p-1)^{-1})$$

and

$$T_0(C(u_0)) = (1-\pi)p\beta^{-2}(p-1)^{-1}.$$

Adding these last two equations, we obtain $D_2(\alpha) = -(\pi^2-1)\beta^{-2}$. Hence (20) holds for $k=2$ and this choice of α, and so the proof of Lemma 12 is complete.

We now establish a remarkable connection between the homomorphisms δ_k, on the one hand, and Leopoldt's Γ-transform, on the other hand. For a similar idea, see the paper by Katz (1977b). This connection is the key to the proof of Theorem 1. We need a slightly more general version of the Γ-transform than that given by Leopoldt, and we refer to Lichtenbaum (to appear) for a complete discussion of this generalization. Here we only state, without proof, the results we shall use from Lichtenbaum (to appear). As in the Introduction, let $\Omega_{\mathfrak{p}}$ be the completion of the maximal unramified extension of $K_{\mathfrak{p}}$, and let $\mathscr{I}_{\mathfrak{p}}$ denote the ring of integers of $\Omega_{\mathfrak{p}}$. Write $|\ |_{\mathfrak{p}}$ for the valuation of $\Omega_{\mathfrak{p}}$, normalized so that $|p|_{\mathfrak{p}} = p^{-1}$. Let v be an indeterminate, and let M denote the subring of $\Omega_{\mathfrak{p}}[[v]]$ consisting of all power series $h = \sum_{n=0}^{\infty} a_n v^n$ satisfying $|n!\,a_n|_{\mathfrak{p}} \to 0$ as $n \to \infty$. We can make M into a normed vector space by defining $\|h\| = \max|n!\,a_n|_{\mathfrak{p}}$. Write $\mathscr{F}$ for the set of continuous functions on $\mathbf{Z}_p$ with values in $\Omega_{\mathfrak{p}}$. Thus $\mathscr{F}$ is also a normed vector space if we endow it with the supremum norm. Let j denote an arbitrary residue class modulo $(p-1)$. Following Leopoldt (1975), Lichtenbaum (to appear) has shown that there is a unique continuous linear map

$$J_j\colon M \to \mathscr{F}$$

satisfying

$$J_j(h)(k) = \left(\frac{d}{dz}\right)^k \tilde{h}(e^z-1)\Big|_{z=0} \tag{26}$$

for all non-negative integers k with $k \equiv j$ modulo $(p-1)$. Here $\tilde{h}(v)$ is defined by the formula

$$\tilde{h}(v) = h(v) - p^{-1}\sum_{\zeta} h(\zeta(v+1)-1), \tag{27}$$

where the sum on the right is taken over all p-th roots of unity ζ. Apart from the existence of the map J_j, we shall need only one additional property of it. Recall that γ_0 denotes our fixed topological generator of the Galois group Γ, and that $u = \kappa(\gamma_0)$. We shall say that a function $f(s)$ in $\mathscr{F}$ is an Iwasawa function if there exists a power series $g(w)$ in $\mathscr{I}_{\mathfrak{p}}[[w]]$ such that $f(s) = g(u^s-1)$ for all s in $\mathbf{Z}_p$.

LEMMA 13. *If h is in $\mathscr{I}_{\mathfrak{p}}[[v]]$, then $J_j(h)$ is an Iwasawa function.*

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

For the proof of this lemma, see Lichtenbaum (to appear). A discussion of these basic properties of the Γ-transform is also given in Lang (to appear).

Let G_m denote the formal multiplicative group. Since E is a formal group of height 1 over $\mathbf{Z}_p$, it is shown in Lubin (1964) that there is an isomorphism

$$\eta\colon G_m \xrightarrow{\sim} \mathrm{E}, \tag{28}$$

which is defined over the ring $\mathscr{J}_{\mathrm{p}}$ of integers of Ω_{p}. We fix one such isomorphism η. Recall that φ denotes the exponential map of E. We see easily that there exists a unique unit γ in $\mathscr{J}_{\mathrm{p}}$ such that

$$w = \varphi(z) = \eta(e^{\gamma z}-1). \tag{29}$$

We write $w_1 * w_2$ for the sum of two elements w_1 and w_2 under the group law of E.

LEMMA 14. *Given $g(w)$ in $\mathscr{J}_{\mathrm{p}}[[w]]$, define $h(v) = g(\eta(v))$. Let $\tilde{h}(v)$ be given by* (27). *Then, for each integer $k \geqslant 0$, we have*

$$\left(\frac{d}{dz}\right)^k \tilde{h}(e^z-1)\bigg|_{z=0} = \gamma^{-k}\left(\frac{d}{dz}\right)^k (g(w)-p^{-1}\sum_{b\in \mathrm{E}_\pi} g(w*b))\bigg|_{z=0}$$

PROOF. Let ζ be a p-th root of unity, and let $b = \eta(\zeta-1)$ be the corresponding point in E_π under the isomorphism (28). Recall that w and z are related by (29). Since η is a group homomorphism, and $\zeta e^{\gamma z}-1$ is the product of $\zeta-1$ and $e^{\gamma z}-1$ on G_m, it follows that

$$\eta(\zeta e^{\gamma z}-1) = \eta(\zeta-1)*\eta(e^{\gamma z}-1) = b*w.$$

Thus, by the chain rule,

$$\gamma^{-k}\left(\frac{d}{dz}\right)^k g(w*b)\bigg|_{z=0} = \left(\frac{d}{dz}\right)^k g(\eta(\zeta e^z-1))\bigg|_{z=0},$$

and so the assertion of the lemma is plain from (27).

LEMMA 15. *Given $g(w)$ in $\mathscr{J}_{\mathrm{p}}[[w]]$ and b in E_π, then, for each integer $k \geqslant 0$, we have*

$$\left(\frac{d}{dz}\right)^k g(w*b)\bigg|_{w=0} = \left(\frac{d}{dz}\right)^k g(w)\bigg|_{w=b}$$

PROOF. By the chain rule, it suffices to verify that, for each integer $k \geqslant 0$, we have

$$\left(\frac{d}{dz}\right)^k (w*b)\bigg|_{w=0} = \left(\frac{d}{dz}\right)^k w\bigg|_{w=b} \tag{30}$$

To this end, let z_1 be a variable independent of z, and put $w_1 = \varphi(z_1)$. Thus

$w * w_1 = \varphi(z+z_1)$. It is now obvious that

$$\left(\frac{\partial}{\partial z}\right)^k (w * w_1)\Big|_{w=0} = \left(\frac{d}{dz}\right)^k w\Big|_{w=w_1},$$

whence (30) is plain on taking $w_1 = b$.

We now return to the situation described earlier in this section. Let i be a fixed, non-zero, residue class modulo $(p-1)$. Let $\alpha = (\alpha_n)$ be an arbitrary element of $X_\infty^{(i)}$, and let $f_\alpha(w)$ be the unique power series in Λ satisfying $f_\alpha(u_n) = \alpha_n$ for all $n \geqslant 0$. Then, as is explained at the beginning of this section,

$$g_\alpha(w) = \frac{d}{dz}\log f_\alpha(w) = f'_\alpha(w)/(f_\alpha(w)\,\lambda'(w)) \tag{31}$$

also belongs to Λ. We further define

$$h_\alpha(v) = g_\alpha(\eta(v)), \tag{32}$$

where η is the isomorphism (28).

THEOREM 16. *Assume that* $i \neq 0$ *modulo* $(p-1)$. *Let* $\alpha = (\alpha_n)$ *be an arbitrary element of* $X_\infty^{(i)}$, *and let* $f_\alpha(w)$ *be the power series in* Λ *satisfying* $f_\alpha(u_n) = \alpha_n$ *for all* $n \geqslant 0$. *Define* $h_\alpha(v)$ *by equations* (31) *and* (32). *Then, for all integers* $k \geqslant 0$ *with* $k \equiv i-1$ *modulo* $(p-1)$, *we have*

$$J_{i-1}(h_\alpha)(k) = \gamma^{-k}\left(1 - \frac{\psi(\mathfrak{p})^{k+1}}{N\mathfrak{p}}\right)\delta_{k+1}(\alpha). \tag{33}$$

PROOF. Combining Lemmas 14 and 15, we obtain

$$\left(\frac{d}{dz}\right)^k \tilde{h}_\alpha(e^z - 1) = \gamma^{-k}(1-p^{-1})\,\delta_{k+1}(\alpha) - \gamma^{-k} p^{-1} D_{k+1}(\alpha),$$

and so (33) follows from (26) and Lemma 12. This completes the proof of the theorem.

COROLLARY 17. *The notation being the same as in Theorem* 16, *there exists an Iwasawa function* $q_\alpha(s)$ *such that, for all integers* $k \geqslant 0$ *with* $k \equiv i-1$ *modulo* $(p-1)$, *we have*

$$q_\alpha(k) = \gamma^{-k}\left(1 - \frac{\psi(\mathfrak{p})^{k+1}}{N\mathfrak{p}}\right)\delta_{k+1}(\alpha).$$

PROOF. This is immediate from Lemma 13 and Theorem 16.

We now make a special choice of $\alpha = (\alpha_n)$ in $X_\infty^{(i)}$. Take $\mathfrak{s} = (A, \mathcal{N})$ to be an arbitrary element of the index set $\mathcal{S}$. Then, by Lemma 9,

$$\beta(\mathfrak{s}) = (\Lambda(\tau_n, \mathfrak{s})^{e_i})$$

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

belongs to $X_\infty^{(i)}$. Moreover, by Theorem 10, the corresponding power series is given by $R(w, \mathfrak{s})^{(i)}$. For $\alpha = \beta(\mathfrak{s})$, the value $\delta_k(\alpha)$ is given by (21) for all integers $k \geqslant 0$ with $k \equiv i$ modulo $(p-1)$. We conclude from Corollary 17 that there exists a unique power series $r_i(w;\, \mathfrak{s})$ in $\mathscr{I}_\mathfrak{p}[[w]]$ satisfying

$$r_i(u^k - 1;\, \mathfrak{s}) = \gamma^{-k}\mu_{k+1} h_{k+1}(\mathfrak{s})\left(1 - \frac{\psi(\mathfrak{p})^{k+1}}{N\mathfrak{p}}\right) L(\bar{\psi}^{k+1}, k+1)$$

for all integers $k \geqslant 0$ with $k \equiv i-1$ modulo $(p-1)$. Here $h_k(\mathfrak{s})$ is given by (10), and μ_k by (2). It is convenient to make a change of variable in the power series $r_i(w;\, \mathfrak{s})$. Put

$$b_i(w;\, \mathfrak{s}) = r_i(u^{-1}(w+1) - 1;\, \mathfrak{s}). \tag{34}$$

Clearly $b_i(w;\, \mathfrak{s})$ also belongs to $\mathscr{I}_\mathfrak{p}[[w]]$, and satisfies

$$b_i(u^k - 1;\, \mathfrak{s}) = \gamma^{1-k}\mu_k h_k(\mathfrak{s})\left(1 - \frac{\psi(\mathfrak{p})^{k}}{N\mathfrak{p}}\right) L(\bar{\psi}^{k}, k) \tag{35}$$

for all integers $k \geqslant 0$ with $k \equiv i$ modulo $(p-1)$.

We can also interpret the numbers $h_k(\mathfrak{s})$, for $k \equiv i$ modulo $(p-1)$, as the values of an Iwasawa function. If x is any unit in $K_\mathfrak{p}$, we write, as usual, $x = \omega(x)\langle x\rangle$, where $\omega(x)$ is a $(p-1)$-th root of unity, and $\langle x\rangle \equiv 1 \bmod \mathfrak{p}$. Since $(\psi(\mathfrak{a}_j)) = \mathfrak{a}_j$, and $\mathfrak{a}_j$ is prime to $\mathfrak{p}$ by hypothesis, the number $\psi(\mathfrak{a}_j)$ is a unit in $K_\mathfrak{p}$ when viewed under the canonical inclusion of K in $K_\mathfrak{p}$. Define $\tau(\mathfrak{a}_j)$ in $\mathbf{Z}_p$ by the equation

$$\langle\psi(\mathfrak{a}_j)\rangle = u^{\tau(\mathfrak{a}_j)}.$$

We then define $a_i(w;\, \mathfrak{s})$ in Λ by the equation

$$a_i(w;\, \mathfrak{s}) = \sum_{j\in J} n_j(N\mathfrak{a}_j - \omega^i(\psi(\mathfrak{a}_j))(1+w)^{\tau(\mathfrak{a}_j)}). \tag{36}$$

Clearly $a_i(u^k - 1;\, \mathfrak{s}) = h_k(\mathfrak{s})$ for all integers $k \geqslant 0$ with $k \equiv i$ modulo $(p-1)$. Write $\mathscr{S}_i$ for the subset of $\mathscr{S}$ consisting of all $\mathfrak{s}$ such that $a_i(w;\, \mathfrak{s})$ is not identically zero. Note that $\mathscr{S}_i$ is certainly non-empty. In fact, since $i \not\equiv 0$ modulo $(p-1)$, Lemma 28 of Coates–Wiles (1977) shows that we can choose $\mathfrak{s}$ in $\mathscr{S}$ such that $a_i(u^k - 1;\, \mathfrak{s})$ is a unit in $K_\mathfrak{p}$, and thus $a_i(w;\, \mathfrak{s})$ is itself a unit in Λ. Given $\mathfrak{s}$ in $\mathscr{S}_i$, we define

$$G_i(w) = b_i(w;\, \mathfrak{s})/a_i(w;\, \mathfrak{s}). \tag{37}$$

It is plain from (35) and (36) that $G_i(u^k - 1)$ is given by equation (38) below for all integers $k \geqslant 0$ with $k \equiv i$ modulo $(p-1)$. In particular, as the right-hand side of (38) is independent of the choice of $\mathfrak{s}$ in $\mathscr{S}_i$, and $G_i(u^s - 1)$ is a continuous function, it follows that $G_i(w)$ itself is independent of the choice of $\mathfrak{s}$ in $\mathscr{S}_i$. Since we can choose $\mathfrak{s}$ in $\mathscr{S}_i$ such that $a_i(w;\, \mathfrak{s})$ is a unit in Λ, we have therefore proven the following theorem.

THEOREM 18. *Assume that* $i \not\equiv 0$ *modulo* $(p-1)$. *Then there exists a power series* $G_i(w)$ *in* $\mathscr{I}_{\mathfrak{p}}[[w]]$ *satisfying*

$$G_i(u^k-1) = \gamma^{1-k}\mu_k\left(1-\frac{\psi(\mathfrak{p})^k}{N\mathfrak{p}}\right)L(\bar{\psi}^k, k) \tag{38}$$

for all integers $k \geqslant 0$ *with* $k \equiv i$ *modulo* $(p-1)$.

For a more detailed study of these functions, see Cassou-Nogues (to appear).

5. Proof of Theorem 1

We now relate the power series $G_i(w)$, constructed in the previous section, to the Iwasawa module

$$Y_\infty^{(i)} = \varprojlim U_n^{(i)}/\bar{C}_n^{(i)},$$

where the projective limit is taken relative to the norm maps. Throughout, we suppose that i is an arbitrary, non-zero, residue class modulo $(p-1)$.

As before, let β be the unique $(p-1)$-th root of $1-\pi$ satisfying $\beta \equiv 1 \bmod p$, and let $\theta_n = (\beta - u_n)^{e_i}$ for all $n \geqslant 0$. Then, by Theorem 4, $\theta = (\theta_n)$ is a basis of $X_\infty^{(i)}$ over Λ. After making a change of variable similar to that in (34), we conclude from Corollary (17) that there is a unique power series $H_i(w)$ in $\mathscr{I}_{\mathfrak{p}}[[w]]$ satisfying

$$H_i(u^k-1) = \gamma^{1-k}\left(1-\frac{\psi(\mathfrak{p})^k}{N\mathfrak{p}}\right)\delta_k(\theta) \tag{39}$$

for all integers $k \geqslant 0$ with $k \equiv i$ modulo $(p-1)$.

LEMMA 19. $H_i(w)$ *is a unit in* $\mathscr{I}_{\mathfrak{p}}[[w]]$.

PROOF. Without loss of generality, we can suppose that i is an integer satisfying $1 \leqslant i < p-1$. Then, by formula (24), $\delta_i(\theta) = -(i-1)!\,\beta^{-i}$. Also, the Euler factor $1-\psi(\mathfrak{p})^i/N\mathfrak{p}$ is obviously a unit in $K_{\mathfrak{p}}$ if $1 < i < p-1$. It is also a unit for $i=1$, because p is not anomalous for E, by hypothesis. Hence $H_i(u^i-1)$ is a unit in $\mathscr{I}_{\mathfrak{p}}$, and thus $H_i(w)$ is a unit in $\mathscr{I}$ $[[w]]$, as required.

For each $\mathfrak{s}$ in $\mathscr{S}$, let $\beta(\mathfrak{s})$ be the element of $X_\infty^{(i)}$ given by $\beta(\mathfrak{s}) = (\Lambda(\tau_n, \mathfrak{s})^{e_i})$. We define $D_\infty^{(i)}$ to be the Λ-submodule of $X_\infty^{(i)}$, which is generated as a Λ-module by the $\beta(\mathfrak{s})$ for $\mathfrak{s}$ ranging over $\mathscr{S}$. In fact, it is plain that $D_\infty^{(i)}$ is a Λ-submodule of $\bar{C}_\infty^{(i)} = \varprojlim \bar{C}_n^{(i)}$.

THEOREM 20. *Assume that* $i \not\equiv 0$ *modulo* $(p-1)$. *Then*

$$D_\infty^{(i)} = \Lambda\mathscr{G}_i(T)\,\theta, \tag{40}$$

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

where $\mathscr{G}_i(T)$ is a power series in Λ, which generates the same ideal in $\mathscr{I}_\mathfrak{p}[[T]]$ as the power series $G_i(T)$ appearing in Theorem 18.

Proof. Let $\mathfrak{s}$ be an arbitrary element of $\mathscr{S}$. Since θ is a Λ-basis of $X_\infty^{(i)}$, there is a uniquely determined power series $\varphi(T, \mathfrak{s})$ in Λ such that

$$\beta(\mathfrak{s}) = \varphi(T, \mathfrak{s})\,\theta.$$

Applying the homomorphism δ_k to both sides of this equation, and recalling (18), we conclude that

$$\delta_k(\beta(\mathfrak{s})) = \varphi(u^k - 1, \mathfrak{s})\,\delta_k(\theta)$$

for all integers $k \geqslant 0$ with $k \equiv i$ modulo $(p-1)$. It now follows from (21), (35) and (39) that

$$b_i(u^k - 1;\, \mathfrak{s}) = \varphi(u^k - 1, \mathfrak{s})\,H_i(u^k - 1)$$

for all integers $k \geqslant 0$ with $k \equiv i$ modulo $(p-1)$. Recalling (37) and Lemma 19, we deduce that

$$\varphi(T, \mathfrak{s}) = G_i(T)\,a_i(T;\, \mathfrak{s})\,H_i(T)^{-1}. \tag{41}$$

This last equation holds for all $\mathfrak{s}$ in $\mathscr{S}$. But now choose $\mathfrak{s}'$ in $\mathscr{S}$ such that $a_i(T;\, \mathfrak{s}')$ is a unit in Λ. We deduce from (41) that $\varphi(T, \mathfrak{s}')$ divides $\varphi(T, \mathfrak{s})$ in Λ, for each $\mathfrak{s}$ in $\mathscr{S}$. It is therefore plain that $D_\infty^{(i)} = \Lambda\varphi(T, \mathfrak{s}')\,\theta$. Moreover, (41) also implies that $\varphi(T, \mathfrak{s}')$ generates the same ideal in $\mathscr{I}_\mathfrak{p}[[T]]$ as $G_i(T)$. Thus we can take $\mathscr{G}_i(T)$ to be $\varphi(T, \mathfrak{s}')$, and the proof of the theorem is complete.

Corollary 21. *Put $Z_\infty^{(i)} = X_\infty^{(i)}/D_\infty^{(i)}$. Then $Z_\infty^{(i)}$ is isomorphic as a Λ-module to $\Lambda/(\mathscr{G}_i(T))$.*

We can now complete the proof of Theorem 1. Indeed, in view of Corollary 21, Theorem 1 is a consequence of the following result.

Theorem 22. *Assume that $i \not\equiv 0$ modulo $(p-1)$. Let $Z_\infty^{(i)} = X_\infty^{(i)}/D_\infty^{(i)}$. For each $n \geqslant 0$, $Z_\infty^{(i)}/\omega_n Z_\infty^{(i)}$ is isomorphic as a Λ-module to $U_n^{(i)}/\bar{C}_n^{(i)}$. In particular, $Y_\infty^{(i)} = \varprojlim U_n^{(i)}/\bar{C}_n^{(i)}$ is isomorphic as a Λ-module to $Z_\infty^{(i)}$.*

Proof. For each $n \geqslant 0$, let $p_n\colon X_\infty^{(i)} \to U_n^{(i)}$ be the canonical projection. By Lemma 2, p_n is surjective, and its kernel is precisely $\omega_n X_\infty^{(i)}$. Moreover, it is clear from the definitions of C_n and $D_\infty^{(i)}$ that

$$p_n(D_\infty^{(i)}) = \bar{C}_n^{(i)}. \tag{42}$$

Let j_n be the composition of p_n with the canonical surjection of $U_n^{(i)}$ onto $U_n^{(i)}/\bar{C}_n^{(i)}$. Thus j_n is surjective. Also, in view of (42), it is plain that the kernel of j_n is precisely

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press

$D_{\infty}^{(i)}\,\omega_n X_{\infty}^{(i)}$. Also j_n is a Λ-homomorphism. But

$$Z_{\infty}^{(i)}/\omega_n Z_{\infty}^{(i)} = X_{\infty}^{(i)}/(D_{\infty}^{(i)}\,\omega_n X_{\infty}^{(i)}).$$

The first assertion of Theorem 22 is therefore clear, and the second assertion follows on passing to the projective limit. This completes the proof of Theorem 22.

References

P. Cassou-Nogues (to appear), "p-adic L-functions for elliptic curves with complex multiplication I."

J. Coates (1977), "p-adic L-functions and Iwasawa's theory", in *Algebraic Number Fields*, edited by A. Frohlich (Academic Press, New York).

J. Coates and A. Wiles (1977), "On the conjecture of Birch and Swinnerton-Dyer", *Invent. Math.* **39**, 223–251.

R. Coleman (to appear), "Some modules attached to Lubin–Tate groups".

K. Iwasawa (1964), "On some modules in the theory of cyclotomic fields", *J. Math. Soc. Japan* **16**, 42–82.

K. Iwasawa (1969), "On p-adic L-functions", *Ann. Math.* **89**, 198–205.

N. Katz (1977), "The Eisenstein measure and p-adic interpolation", *Amer. J. Math.* **99**, 238–311.

N. Katz (1977), "Formal groups and p-adic interpolation", *Asterisque* **41–42**, 55–65.

S. Lang, *Introduction to Cyclotomic Fields* (to be published by Springer Verlag).

H. Leopoldt (1975), "Eine p-adische Theorie der Zetawerte II", *J. reine angew. Math.* **274–275**, 224–239.

S. Lichtenbaum (to appear), "On p-adic L-functions associated to elliptic curves".

J. Lubin (1964), "One parameter formal Lie groups over p-adic integer rings", *Ann. Math.* **80**, 464–484.

J. Manin and M. Vishik (1974), "p-adic Hecke series for imaginary quadratic fields", *Math. Sbornik* **95**, 357–383.

G. Robert (1973), "Unités elliptiques", *Bull. Soc. Math. France Mémoire* **36**.

G. Shimura (1971), *Introduction to the Arithmetic Theory of Automorphic Functions* (Pub. Math. Soc. Japan) **11**, 1971.

A. Wiles (1978), "Higher explicit reciprocity laws", *Ann. Math.*, **107**, 235–254.

Department of Mathematics
Institute of Advanced Studies
Australian National University
Canberra, Australia

Department of Mathematics
Harvard University
Cambridge, Mass. 02138, USA

https://doi.org/10.1017/S1446788700011459 Published online by Cambridge University Press