ANNALES DE L'INSTITUT FOURIER

JOHN L. BOXALL

A new construction of p-adic L-functions attached to certain elliptic curves with complex multiplication

Annales de l'institut Fourier, tome 36, n° 4 (1986), p. 31-68

<http://www.numdam.org/item?id=AIF_1986__36_4_31_0>

© Annales de l'institut Fourier, 1986, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
36, 4 (1986), 31-68.

A NEW CONSTRUCTION OF p-ADIC L-FUNCTIONS ATTACHED TO CERTAIN ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

by John L. BOXALL

Introduction.

The purpose of this paper is to use some of the results on p-adic interpolation obtained in an earlier article [1] to construct locally analytic p-adic L-functions associated to certain elliptic curves with comple multiplication. Although our main interest lies with supersingular primes, we shall also consider ordinary primes since our method applies with little change to both cases.

To explain our results, let $p \geqslant 5$ be a prime number, K an imaginary quadratic field, F an extension of K of degree n and $\mathfrak{p}$ a prime ideal of K lying above p. Fix once and for all embeddings of the algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$ into $\mathbf{C}$ and $\mathbf{C}_p$ subject to (13) in § 2. Here $\mathbf{C}_p$ denotes the completion of the algebraic closure of $\mathbf{Q}_p$. If p splits in $K((p) = \mathfrak{p}\bar{\mathfrak{p}}, \bar{\mathfrak{p}} \neq \mathfrak{p})$ we suppose further that the embedding $\bar{\mathbf{Q}} \hookrightarrow \mathbf{C}_p$ is p-adic. If a is an integer of K not divisible by $\mathfrak{p}$ we write $\omega(a)$ for the unique prime-to$-p$-th root of unity in $\mathbf{C}_p$ congruent to a modulo $\mathfrak{p}$. Let E be an elliptic curve defined over F having complex multiplication by the full ring of integers $\mathfrak{O}_K$ of K. Choose a Weierstrass model $y^2 = x^3 + ax + b$ of E over F and let $\mathscr{L}$ be the lattice of periods of the differential $\dfrac{dx}{2y}$ on $E(\mathbf{C})$. We suppose that the following conditions on E, $\mathfrak{p}$ and F are satisfied:

(i) E has good reduction at all the primes of F above $\mathfrak{p}$,

(ii) $F(E_{tors})$ is abelian over K.

Key-words: Fonctions Lp-adiques - Courbes elliptiques.

It is also convenient to assume that

(iii) $\mathscr{L} = \Omega\mathfrak{O}_K$ for some $\Omega \in \mathbf{C}^*$ (which we fix).

It is well-known that this can be satisfied by replacing E by one of its Gal(F/K)-conjugates. If Λ is an arbitrary lattice in $\mathbf{C}$ and $k > 0$ is an integer, we define, for all z, $s \in \mathbf{C}$ with $\mathrm{Re}(s)$ sufficiently large

$$G_k(z,s,\Lambda) = \sum_w{}' \frac{(\bar{z} + \bar{w})^k}{|z+w|^{2s}} \tag{1}$$

where the sum is taken over all $w \in \Lambda$ except $w = -z$ if $z \in \Lambda$. It is known that for fixed k and z, $s \mapsto G_k(z,s,\Lambda)$ has an analytic continuation to the whole complex plane. Let $v: \mathbf{C}_p^* \to \mathbf{Q}$ be the valuation normalised so that $v(p) = 1$. In § 2 we shall prove

THEOREM A. — *Let* $\mathfrak{g}$ *be an integral ideal of* K *divisible by* $\mathfrak{p}$ *and* a *an element of* $\mathfrak{O}_K$ *which is not divisible by* $\mathfrak{p}$. *Let* d_K *be the discriminant of* K *and* Ω *as above. Then there exists a constant* $\Omega_\mathfrak{p} \in \mathbf{C}_p^*$ *and a unique locally meromorphic function* $G_\mathfrak{p}(a,s,\mathfrak{g}) \to \mathbf{C}_p$ *such that*

$$v(\Omega_\mathfrak{p}) = \begin{cases} 0, & \text{if } p \text{ splits in } K\ ((p)=\mathfrak{p}\bar{\mathfrak{p}},\ \bar{\mathfrak{p}} \neq \mathfrak{p}) \\ \dfrac{1}{p-1} - \dfrac{1}{p^2-1}, & \text{if } p \text{ is inert in } K((p)=\mathfrak{p}) \\ \dfrac{1}{2(p-1)}, & \text{if } p \text{ is ramified in } K\ ((p)=\mathfrak{p}^2) \end{cases}$$

and

$$G_\mathfrak{p}(a,k,\mathfrak{g}) = \frac{1}{\Omega_\mathfrak{p}^k}\left[\left(\frac{|d_K|^{\frac{1}{2}}}{2\pi}\right)^{1-k} \frac{G_k(\bar{a},1,\bar{\mathfrak{g}})}{\Omega^k}\, \omega^{-k}(a)\right] \tag{2}$$

for all $k > 0$. *Moreover* $G_\mathfrak{p}(a,s,\mathfrak{g})$ *is locally analytic except at* $s = 0$ *where it has a simple pole with residue* $(N\mathfrak{g})^{-1}$.

The formulation of this theorem is by analogy with Theorem 5.9 of Washington [30] where the p-adic interpolation of partial zeta functions at negative integers is obtained and later used to construct the Kubota-Leopoldt p-adic L-functions. Indeed we shall see in § 3 that Theorem A can be used to construct $\mathfrak{p}$-adic partial zeta functions attached to abelian extensions of K. The appearance of the functions G_k at $s = 1$ rather than $s = k$ may be viewed as analogous to the fact that it is easier to interpolate partial zeta functions at negative rather than positive integers (though they are related via the functional equation).

The algebraicity of $\Omega_p^k \times$ (the right hand since of (2)) follows from a result of Damerell [7] (see also Weil [31, chapters VI and IX]).

In § 3 we apply Theorem A to the construction of p-adic L-functions of E. Let J_F be the idele group of F and A_p the direct sum of the components of the idele A at the primes of F above p. Let ψ: $J_F \to K^*$ be the Hecke character attached to E over F as in Serre-Tate [26, Theorem 10], and ε: $\mathrm{Gal}(\bar{\mathbf{Q}}/F) \to K_p^*$ the character giving the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/F)$ on the p-division points of E. Here K_p is the completion of the image of K in $\mathbf{C}_p$ and K_p^* its multiplicative group. Clearly ε factors through to a character of $\mathrm{Gal}(F(E_p)/F)$ and so can be viewed as a character of J_F via class field theory. We shall see (Proposition 8(i)) that the conductor of $\psi\varepsilon^{-1}$ is divisible at most by primes above p. Since ε is of finite order $\psi\varepsilon^{-1}$ takes values in $\bar{\mathbf{Q}}^*$; therefore if θ: $\mathrm{Gal}(F^{ab}/F) \to \bar{\mathbf{Q}}^*$ is a character of finite order (again viewed as a character on J_F) we can define, for each integer $k \geqslant 1$, the complex L-series

$$L^*((\psi\varepsilon^{-1})^k,\theta,s) = \sum_{\mathfrak{A}} \frac{(\psi\varepsilon^{-1})^k(\mathfrak{A})\theta(\mathfrak{A})}{N\mathfrak{A}^s}$$

where the sum is taken over all ideals A of F prime to p and the conductor of θ. The asterisk is used to indicate that the Euler factors for primes above p have been omitted. We shall prove

THEOREM B. — *Let notation be as above and suppose in addition that* θ *factors through a character of* $\mathrm{Gal}(K^{ab}/F)$. *Then there is a unique locally meromorphic function* $L_p(\psi,\theta,s)$: $\mathbf{Z}_p \to \mathbf{C}_p$ *such that*

$$L_p(\psi,\theta,k) = \frac{1}{\Omega_p^{kn}}\left[\left(\left(\frac{|d_K|^{\frac{1}{2}}}{2\pi}\right)^{1-k}\frac{1}{\Omega^k}\right)^n L^*(\psi\varepsilon^{-1})^k,\theta,1)\right]$$

whenever $k \geqslant 1$. *Moreover* $L_p(\psi,\theta,s)$ *is locally analytic except when* θ *is trivial, in which case the only singularity is a simple pole at* $s = 0$.

In particular taking $\theta = \varepsilon$; we obtain a function $L_p(E/F,s)$ which deserves to be called the p-adic L-function of E over F. It has a pole at $s = 0$ if and only if $F(E_p) = F$.

The proof of Theorem B is given in § 3 and § 4. In § 4 we also discuss p-adic Kronecker limit formulae at $s = 0$ for some of the function discussed in § 3, and use this to outline the existence of the pole of $L_p(\psi,\theta,s)$ at $s = 0$ when θ is trivial.

p-adic L-functions of one and several variables associated to elliptic curves with complex multiplication were introduced by Vishik-Manin [29] and then studied by Katz [13], [14], Lichtenbaum [19], Coates-Wiles [6] and many others. For recent versions see Coates-Goldstein [4], Yager [32], [33], de Shalit [27]. Moreover very recent work of Colmez and Schneps should enable one to suppress the restriction that $F(E_{tors})$ is abelian over K. A quite different idea valid for any so-called Weil curve, was introduced by Mazur-Wiles [22]. All the above authors confine their attention to ordinary primes, but the treatment involving partial zeta functions associated to abelian extensions of K appears to be new. In a subsequent paper [2], we shall show how to construct Iwasawa functions from these partial zeta functions. As for supersingular primes, the literature seems to be confined to Katz [15], [16] and Rubin [24]. Although these authors confine their attention to elliptic curves over K they obtain congruences between the values of the L-series which seem to be difficult to derive using the methods developped in [1] and the present paper. Finally it should be mentioned that nothing seems to be known about two-variable p-adic L-functions in the supersingular case.

Acknowledgements.

An earlier version of this paper first appeared as part of my Oxford D Phil Thesis, and I would like to thank the SERC for its financial support during its preparation. I would also like to thank my research supervisor Dr. B. J. Birch, as well as J. Tilouine, N. Schappacher and G. Robert for their interest in my work.

1. Notation and Results Needed form [1].

As in the Introduction, let $p \geqslant 5$ be a prime number, K an imaginary quadratic field, F an extension of degree n of K and $\mathfrak{p}$ a prime ideal of K lying above p. Let $\mathfrak{O}_K$ be the ring of integers of K, e the ramification index of p in K and q the number of elements of the residue field $\mathfrak{O}_K/\mathfrak{p}$. Let $\mathbf{C}_p$ denote the completion of the algebraic closure of $\mathbf{Q}_p$, $\mathfrak{O}$ be its ring of integers and $\mathfrak{m}$ its maximal ideal. We fix embeddings of the algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$ into $\mathbf{C}$ and $\mathbf{C}_p$ subject to (13) in § 2. If in addition p splits in K, we require the embedding $\bar{\mathbf{Q}} \hookrightarrow \mathbf{C}_p$ to be p-adic. Let E be an elliptic curve defined over F having complex multiplication by $\mathfrak{O}_K$. Fix a Weierstrass model $y^2 = x^3 + ax + b$ of E over F and let $\mathscr{L}$ be the lattice of periods of the differential $\dfrac{dx}{2y}$ on

$E(\mathbf{C})$. We suppose that the conditions (i), (ii) and (iii) are satisfied. In particular condition (ii) implies that F/K is abelian and that E is isogeneous over F to each of its $\mathrm{Gal}(F/G)$-conjugates (see [9, § 4]). If $\mathfrak{a}$ is an integral ideal of K, $E_{\mathfrak{a}}$ denotes the group of $\mathfrak{a}$-torsion points of E and $E_{\mathfrak{a}\mathfrak{p}^\infty} = \bigcup_{n=1}^{\infty} E_{\mathfrak{a}\mathfrak{p}^n}$.

Let $K_{\mathfrak{p}}$ (resp. $F_{\mathfrak{p}}$) denote the completion of the image of K (resp. F) in $\mathbf{C}_p$ and let $\mathfrak{O}_{K_{\mathfrak{p}}}$ (resp. $\mathfrak{O}_{F_{\mathfrak{p}}}$) be the ring of integers of $K_{\mathfrak{p}}$ (resp. $F_{\mathfrak{p}}$). If $a \in \mathfrak{O}_{K_{\mathfrak{p}}}^*$, the group of invertible elements of $\mathfrak{O}_{K_{\mathfrak{p}}}$, we denote by $\omega(a)$ the unique root of unity in $K_{\mathfrak{p}}$ congruent to a (modulo $\mathfrak{p}$). Let $\hat{E}$ be the formal group of E, – it is defined over $\mathfrak{O}_{F_{\mathfrak{p}}}$. If π denotes a uniforming parameter of $K_{\mathfrak{p}}$, and $\mathfrak{F}_0$ is the basic Lubin-Tate formal group associated to the polynomial $\pi X + X^q$, then our hypothesis on E imply that $\hat{E}$ is isomorphic to $\mathfrak{F}_0$ over $\mathfrak{O}$. This allows us to apply the results of [1] which we now recall. Let $\hat{\mathbf{G}}_m$ denote the multiplicative group. According to a result of Tate [28] (see also [1, § 1], $\mathrm{Hom}_{\mathfrak{O}}(\hat{E},\hat{\mathbf{G}}_m)$ is a free $\mathfrak{O}_{K_{\mathfrak{p}}}$-module of rank one. Fix a generator $t_1 \in \mathfrak{O}[[T]]$. We denote by $+_{\hat{E}}$ the operation of the addition law on $\hat{E}$ on power series or on elements of $\mathfrak{m}$. Thus $\mathrm{Hom}_{\mathfrak{O}}(\hat{E},\hat{\mathbf{G}}_m) = \{f(T) \in \mathfrak{O}[[T]] \mid f(X +_{\hat{E}} Y) = f(X)f(Y) \text{ and } f(0) = 1\}$. If $a \in \mathfrak{O}_{K_{\mathfrak{p}}}$ we denote by $[a]$ the corresponding endomorphism of $\hat{E}$ and write t_a for $t_1 \circ [a]$. Define a constant $\Omega_{\mathfrak{p}} \in \mathbf{C}_p^*$ by

$$t_a(T) = 1 + \Omega_{\mathfrak{p}} a T + O(T^2).$$

It is shown in [1, § 4] that under our hypotheses

$$v(\Omega_{\mathfrak{p}}) = \frac{1}{p-1} - \frac{1}{e(q-1)},$$

and our proof of Theorem A will show that the $\Omega_{\mathfrak{p}}$ appearing there is in fact the same as this one.

Let λ denote the logarithm of $\hat{E}$, i.e. the unique element of $F_{\mathfrak{p}}[[T]]$ satisfying $\lambda(X +_{\hat{E}} Y) = \lambda(X) + \lambda(Y)$ and $\lambda(T) = T + O(T^2)$. It is well-known that $\lambda'(T) \in 1 + T\mathfrak{O}[[T]]$. Define a differential operator D_1 on $\mathbf{C}_p[[T]]$ by $(D_1 f)(T) = \frac{1}{\lambda'(T)} f'(T)$. Thus D_1 takes elements of $\mathfrak{O}[[T]]$ to elements of $\mathfrak{O}[[T]]$ and if $z = \lambda(T)$, then

$$D_1 = \frac{d}{dz}.$$

Let $B = \{f \in \mathbf{C}_p[[T]] \mid \exists r \geqslant 0$ such that $D_1^r f \in \mathfrak{O}[[T]]\}$, (we adopt the convention that $D_1^r f = f$ if $r = 0$). Fix a non-trivial element η_0 of $\ker[\pi]$, so that $\ker[\pi] = \{[c](\eta_0)\}$ where c runs over a complete set of representatives of $\mathfrak{O}_{K_p}$ modulo π. Let $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$ with $\beta \neq 0$, and define

$$\tau_a(\beta) = \sum_u{}' \omega^\beta(u) t_a([u](\eta_0))$$

and

$$\tau(\beta) = \tau_1(\beta)$$

where the sum runs over a complete set of representatives of $\mathfrak{O}_{K_p}^*$ modulo π. By Lemma 3 of [1] we have

$$\tau_a(\beta) = \omega^{-\beta}(a)\tau(\beta) \quad \text{if} \quad a \in \mathfrak{O}_{K_p}^*$$

and

$$\tau(\beta)\tau(-\beta) = (-1)^\beta q.$$

For each $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$, we define an operator $\Delta^{(\beta)}$ on B by

$$\begin{aligned}(\Delta^{(\beta)}f)(T) &= f(T) - \frac{1}{q}\sum_u f(T +_{\hat{E}} [u](\eta_0)) \quad \text{if} \quad \beta = 0 \\ &= \frac{\tau(\beta)}{q}\sum_u{}' f(T +_{\hat{E}} [u](\eta_p))\omega^{-\beta}(u) \quad \text{if} \quad \beta \neq 0,\end{aligned}$$

where the first (resp. second) sum is taken over a complete set of representatives of $\mathfrak{O}_{K_p}$ (resp. $\mathfrak{O}_{K_p}^*$) modulo π. This is well-defined, since B is in fact contained in the ring B_0 discussed in § 1 of [1]. According to Lemma 5 of [1], B can be decomposed into eigenspaces for the $\Delta^{(\beta)}$s. More precisely, if $f \in B$ and $a \in \mathfrak{O}_{K_p}$, then we define

$$F_a(T) = \sum_{\eta \in \ker[\pi]} f(T +_{\hat{E}} \eta) t_a(\eta); \tag{3}$$

we have

$$\begin{aligned}(\Delta^{(\beta)}F_a)(T) &= \omega^\beta(a)F_a(T) \quad \text{if} \quad a \not\equiv 0 \pmod{\pi} \\ &= 0 \quad \text{if} \quad a \equiv 0 \pmod{\pi}.\end{aligned} \tag{4}$$

We shall need the following interpolation theorem, which is Corollary 12 of [1]:

THEOREM 1. — *Let* $f \in B$ *and* $\alpha \in \mathbf{Z}/(q-1)\mathbf{Z}$. *Then there exists a unique locally analytic function* $C_f^{(\alpha)}: \mathbf{Z}_p \to \mathbf{C}_p$ *such that for each*

$\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$

$$C_f^{(\alpha)}(k) = (-1)^{\alpha-\beta} \frac{D_1^k(\Delta^{(\alpha-\beta)}f)(0)}{\Omega_p^k}$$

whenever $k \geqslant 0$ *and* $k \in \beta$.

Here $C_f^{(\alpha)}$ locally analytic means that it can be expanded in a Taylor series with non-zero radius of convergence about every point of $\mathbf{Z}_p$.

2. Interpolation of Eisenstein Series.

This section is devoted to the proof of Theorem A. We begin by recalling some definitions and results on elliptic functions and Eisenstein series.

Let Λ be a lattice in $\mathbf{C}$. Define as usual

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

$$\zeta(z,\Lambda) = \frac{d}{dz} \log \sigma(z,\Lambda) = \frac{1}{z} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{z+w} - \frac{1}{w} + \frac{z}{w^2}\right)$$

$$\mathscr{P}(z,\Lambda) = -\frac{d}{dz}\zeta(z,\Lambda) = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z+w)^2} - \frac{1}{w^2}\right).$$

Since $\mathscr{P}(z,\Lambda)$ is an elliptic function, $\eta(w,\Lambda) = \zeta(z+w,\Lambda) - \zeta(z,\Lambda)$ is independent of z and the map $w \to \eta(w,\Lambda)$ defines a homomorphism $\Lambda \to \mathbf{C}$ which extends by $\mathbf{R}$-linearity to a map $\mathbf{C} \to \mathbf{C}$ also denoted by $\eta(w,\Lambda)$. We have, if $w \in \Lambda$,

$$\sigma(z+w,\Lambda) = \pm\, \sigma(z,\Lambda) \exp\left(\eta(w,\Lambda)\left(z+\frac{1}{2}w\right)\right) \tag{5}$$

where the sign is taken $+$ or $-$ according as to whether $w \in 2\Lambda$ or not (see [17], Chapter 18, § 1]).

Let ρ, $\hat{\rho} \in \mathbf{C}$ and $a(\Lambda)$ be the « area » of Λ, i.e. the quantity $\left|\frac{w_1\bar{w}_2 - \bar{w}_1 w_2}{2i}\right|$ where w_1 and w_2 are a $\mathbf{Z}$-basis for Λ, and the bar

denotes complex conjugation. We define

$$(6) \qquad <\rho,\hat{\rho}>_\Lambda = \exp\left(\frac{\pi}{a(\Lambda)}(\rho\bar{\hat{\rho}}-\bar{\rho}\hat{\rho})\right)$$

where $\pi = 3.14159\ldots$. If $k \in \mathbf{N}$ and $s \in \mathbf{C}$ with $\mathrm{Re}(s)$ sufficiently large, define

$$(7) \qquad H_k(\rho,\hat{\rho},s,\Lambda) = {\sum_{w\in\Lambda}}' <w,\bar{\rho}>_\Lambda \frac{(\bar{\rho}+\bar{w})^k}{|\rho+w|^{2s}}$$

where the summation is taken over all $w \in \Lambda$ except $w = -\rho$ if $\rho \in \Lambda$. It is known (see Weil [31, VIII, § 13]) that $H_K(\rho,\hat{\rho},s,\Lambda)$ extends to a holomorphic function on the whole of $\mathbf{C}$ and satisfies the functional equation

$$(8) \quad \Gamma(s)H_k(\rho,\hat{\rho},s,\Lambda) = \left(\frac{a(\Lambda)}{\pi}\right)^{1+k-2s} \Gamma(1+k-s)<\rho,\hat{\rho}>_\Lambda^{-1} H_k(\hat{\rho},\rho,1+k-s,\Lambda).$$

Write

$$G_k(\rho,s,\Lambda) = H_k(\rho,0,s,\Lambda)$$
$$G_k(\rho,\Lambda) = G_k(\rho,k,\Lambda)$$

and

$$G_k(\Lambda) = G_k(0,\Lambda);$$

if $k \geqslant 3$ then $G_k(\rho,\Lambda) = \Sigma \dfrac{1}{(\rho+w)^k} = (-1)^k \dfrac{\mathscr{P}^{(k-2)}(\rho,\Lambda)}{(k-1)!}$ provided $\rho \notin \Lambda$. We have the identities

$$\left.\begin{aligned} (9A) \qquad \zeta(z,\Lambda) &= G_1(z,\Lambda) + zG_2(\Lambda) + \frac{\pi\bar{z}}{a(\Lambda)} \\ (9B) \qquad \mathscr{P}(z,\Lambda) &= G_2(z,\Lambda) - G_2(\Lambda) \\ (10) \qquad \eta(z,\Lambda) &= zG_2(\Lambda) + \frac{\pi\bar{z}}{a(\Lambda)} \end{aligned}\right\} z \notin \Lambda$$

(see [9] (1.5) and (1.6)).

Let $\Delta(\Lambda) = (60G_4(\Lambda))^3 - 27(140G_6(\Lambda))^2$ be the discriminant of Λ and define

$$(11) \qquad \theta(z,\Lambda) = \exp(-6G_2(\Lambda)z^2)\,\Delta(\Lambda)\sigma^{12}(z,\Lambda).$$

If, further, Λ' is a lattice containing Λ with index $(\Lambda' : \Lambda)$ we define

$$\theta(z,\Lambda;\Lambda') = \frac{\theta(z,\Lambda)^{(\Lambda':\Lambda)}}{\theta(z,\Lambda')}. \tag{12}$$

LEMMA 2. — (i) $\theta(z,\Lambda;\Lambda')$ *is an elliptic function on* Λ *and in fact*

$$\theta(z,\Lambda;\Lambda') = \frac{\Delta(\Lambda)^{(\Lambda':\Lambda)}}{\Delta(\Lambda')} \prod_{\lambda}{}' (\mathscr{P}(z,\Lambda)-\mathscr{P}(\lambda,\Lambda))^{-6}$$

where the product is taken over a complete set of representatives $\{\lambda\}$ *of the non-zero cosets of* Λ *in* Λ'.

(ii) *We have the Laurent expansions*

$$\frac{d}{dz}\log\theta(z,\Lambda;\Lambda') = \frac{12((\Lambda':\Lambda)-1)}{z} + 12\sum_{k=1}^{\infty}(-1)^{k-1}(G_k(\Lambda)(\Lambda':\Lambda)-G_k(\Lambda'))z^{k-1}$$

and, if $\rho \notin \Lambda$

$$\frac{d}{dz}\log\theta(z+\rho,\Lambda;\Lambda') = 12\sum_{k=1}^{\infty}(-1)^{k-1}(G_k(\rho,\Lambda)(\Lambda':\Lambda)-G_k(\rho,\Lambda'))z^{k-1}.$$

Proof. — (i) The fact that $\theta(z,\Lambda;\Lambda')$ is an elliptic function on Λ follows easily from (5). The explicit formula for it follows from a routine comparison of divisors and ratios as $z \to 0$, and we omit the details.

(ii) We only consider the case $\rho \notin \Lambda$. In view of (11) we have

$$\frac{d}{dz}\log\theta(z+\rho,\Lambda) = -12G_2(\Lambda)(z+\rho) + 12\zeta(z+\rho,\Lambda).$$

Now $\zeta(z+\rho,\Lambda) = \zeta(\rho,\Lambda) + \zeta'(\rho,\Lambda)z + \sum_{k=2}^{\infty}\zeta^{(k)}(\rho,\Lambda)\frac{z^k}{k!}$ and

$$\zeta'(\rho,\Lambda) = -\mathscr{P}(\rho,\Lambda)$$

and

$$\zeta^{(k)}(\rho,\Lambda) = (-1)^k G_{k+1}(\rho,\Lambda)k! \qquad \text{if} \qquad k \geqslant 2.$$

Therefore by (9)

$$\frac{d}{dz}\log\theta(z+\rho,\Lambda) = 12\left(\frac{\pi\bar{\rho}}{a(\Lambda)} + G_1(\rho,\Lambda)\right) + 12\sum_{k=2}^{\infty}(-1)^{k-1}G_k(\rho,\Lambda)z^{k-1}.$$

Comparing this with the similar expression for $\frac{d}{dz}\log\theta(z+\rho,\Lambda')$ and observing that $a(\Lambda) = (\Lambda' : \Lambda)a(\Lambda')$ we obtain (ii).

Our next lemma is a version of the functional equation (8) more suited to our purposes. If Λ' is a lattice containing Λ and $\hat{\rho} \in \Lambda$, then the map $\rho \mapsto <\rho,\hat{\rho}>_\Lambda$ gives rise to a character of the additive group Λ'/Λ. Let Λ'' be the dual lattice of Λ' with respect to Λ, i.e. $\{\rho \in \mathbf{C} \mid <\rho,\hat{\rho}>_\Lambda = 1 \text{ for all } \rho \in \Lambda'\}$. Then Λ'' is clearly a sublattice of Λ with index $(\Lambda' : \Lambda)$.

LEMMA 3. — *With notation as above let* $\hat{\rho} \in \Lambda$ *be fixed. Then for each* $k \geqslant 1$

$$\Gamma(s) \sum_{\rho \bmod \Lambda} G_k(\rho,s,\Lambda) <\rho,\hat{\rho}>_\Lambda = (\Lambda' : \Lambda)\left(\frac{a(\Lambda)}{\pi}\right)^{1+k-2s} \Gamma(1+k-s)G_k(\hat{\rho},1+k-s,\Lambda'')$$

where the sum on the left is taken over a complete set of representatives $\{\rho\}$ *in* $\mathbf{C}$ *of* Λ' *modulo* Λ.

Proof. — For each representative ρ multiply (8) by $<\rho,\hat{\rho}>_\Lambda$ and sum over ρ. Since $\hat{\rho} \in \Lambda$, one has $H_k(\rho,\hat{\rho},s,\Lambda) = G_k(\rho,s,\Lambda)$ so that we obtain

$$\Gamma(s)\Sigma G_k(\rho,s,\Lambda) <\rho,\hat{\rho}>_\Lambda = \left(\frac{a(\Lambda)}{\pi}\right)^{1+k-2s} \Gamma(1+k-s)H_k(\hat{\rho},\rho,1+k-s,\Lambda).$$

Recalling the definition of $H_k(\hat{\rho},\rho,1+k-s,\Lambda)$ from (24) and that

$$\sum_\rho <w,\rho>_\Lambda = (\Lambda' : \Lambda) \quad \text{or} \quad 0$$

according as to whether $w \in \Lambda''$ or not we obtain Lemma 15.

Now let E be our elliptic curve with Weierstrass model $y^2 = x^3 + ax + b$, and $\mathscr{L}$ the lattice of periods of $\frac{dx}{2y}$ on $E(\mathbf{C})$. Let ξ be the analytic isomorphism $\mathbf{C}/\mathscr{L} \to E(\mathbf{C})$ given by $z \mapsto \xi(z) = \left(\mathscr{P}(z,\mathscr{L}), \frac{1}{2}\mathscr{P}'(z,\mathscr{L})\right)$. On the other hand if $\hat{E}$ is the formal group of E and $\hat{E}(\mathfrak{m})_{\text{tors}}$ the torsion subgroup of $\hat{E}(\mathfrak{m})$ then the maps

$$\hat{E}(\mathfrak{m})_{\text{tors}} \twoheadrightarrow E_{p^\infty} \hookrightarrow E(\bar{\mathbf{Q}}) \hookrightarrow E(\mathbf{C}) \overset{\xi}{\leftarrow} \mathbf{C}/\mathscr{L}$$

induce an $\mathfrak{O}_{K_p}$-module isomorphism $\nu : \hat{E}(\mathfrak{m})_{\text{tors}} \to \bigcup_{n=1}^{\infty} \mathfrak{p}^{-n}\mathscr{L}/\mathscr{L}$ which is determined by our embeddings of $\bar{\mathbf{Q}}$ into $\mathbf{C}$ and $\mathbf{C}_p$.

It is convenient to choose the generator t_1 of $\mathrm{Hom}_{\mathfrak{O}}(\hat{E},\hat{\mathbf{G}}_m)$ (or equivalently the embeddings of $\bar{\mathbf{Q}}$ into $\mathbf{C}$ and $\mathbf{C}_p$) in such a way that

$$t_1(\eta) = <\nu(\eta),\Omega>_{\mathscr{L}} \tag{13}$$

for all $\eta \in \hat{E}(\mathfrak{m})_{\text{tors}}$. This is possible since as a runs over $\mathfrak{O}_{K_p}$ so $\eta \mapsto t_a(\eta)$ runs over

$$\mathrm{Hom}_{Z_p}(\hat{E}(\mathfrak{m})_{\text{tors}},\mu_{p^\infty}) \xrightarrow{\sim} \mathrm{Hom}_{Z_p}(\cup\, \mathfrak{p}^{-n}\mathscr{L}/\mathscr{L},\mu_{p^\infty})$$

where μ_{p^∞} denotes the group of p-power roots of unity: and so in particular there exists $a_0 \in \mathfrak{O}_{K_p}$ such that $t_{a_0}(\eta) = <\nu(\eta),\Omega>_{\mathscr{L}}$ for all η. Then $a_0 \not\equiv 0 \pmod{\pi}$ since $\eta \mapsto <\nu(\eta),\Omega>_{\mathscr{L}}$ restricted to $\ker[\pi]$ is non-trivial and so by applying an automorphism of $\mathbf{C}_p/K_p$ we may suppose that $a_0 = 1$.

We shall now begin the proof of Theorem A, deducing it from Theorem 1 by constructing suitable elements of $\mathfrak{O}[[T]]$ with the help of Propositions 4 and 5 below. Let $\mathfrak{g}$ be an integral ideal of K divisible by $\mathfrak{p}$ and Σ the set of integral ideals $\mathfrak{c}$ of K satisfying $\mathfrak{c} \neq (1)$ and $\mathfrak{c}$ is prime to $6N\mathfrak{g} \times$ (the product of the primes of K lying below those of F at which E does not have good reduction). It is convenient to introduce a finite set S of pairs $(\mathfrak{c},a_{\mathfrak{c}})$ with $\mathfrak{c} \in \Sigma$ and $a_{\mathfrak{c}} \in \mathbf{Z}$ satisfying $\sum_{\mathfrak{c}} (N\mathfrak{c}-1)a_{\mathfrak{c}} = 0$.

Let $\rho \in \mathfrak{g}^{-1}\mathscr{L}$ and suppose that $\rho \notin \mathfrak{p}^{-n}\mathscr{L}$ for any $n \in \mathbf{Z}_+$. Then it is well-known (see § 4 and Robert [23]) that $\theta(\rho,\mathscr{L};\mathfrak{c}^{-1}\mathscr{L})$ is a $\mathfrak{p}$-unit of $\bar{\mathbf{Q}}$ for each $\mathfrak{c} \in \Sigma$ and so we can define an element $g(T,\rho,\mathfrak{c})$ of $\mathbf{C}_p[[T]]$ by

$$g(T,\rho,\mathfrak{c}) = \log_p(\theta(\lambda(T)+\rho,\mathscr{L};\mathfrak{c}^{-1}\mathscr{L})). \tag{14}$$

This is to be interpreted as follows: by Lemma 2 (i) $\theta(z+\rho,\mathscr{L};\mathfrak{c}^{-1}\mathscr{L})$ has a Taylor expansion at $z = 0$ with coefficients in $\bar{\mathbf{Q}}$, and constant term a $\mathfrak{p}$-unit, so we may formally substitute $z = \lambda(T)$ and take the p-adic logarithm. If now ρ is an arbitrary element of $\mathfrak{g}^{-1}\mathscr{L}$, then $\prod_{\mathfrak{c}} \theta(\rho,\mathscr{L};\mathfrak{c}^{-1}\mathscr{L})^{a_{\mathfrak{c}}}$ is still a $\mathfrak{p}$-unit and we can apply similar considerations to obtain a power series

$$f(T,\rho,S) = \log_p \prod_{\mathfrak{c}} (\theta(\lambda(T)+\rho,\mathscr{L};\mathfrak{c}^{-1}\mathscr{L})^{a_{\mathfrak{c}}} \tag{15}$$

in $\mathbf{C}_p[[T]]$. Since $\theta(z,\mathscr{L};c^{-1}\mathscr{L})$ is an elliptic function on $\mathscr{L}$ it is clear that the power series (14) and (15) depend only on ρ modulo $\mathscr{L}$. The following proposition is a generalisation of Lemma 21 of [5].

PROPOSITION 4. — *Let* $\rho \in \mathbf{Q}\mathscr{L}$.

(i) *If* $\rho \notin \mathfrak{p}^{-n}\mathscr{L}$ *for all* $n \in \mathbf{Z}_+$ *then* $D_1 g(T,\rho,c) \in \mathfrak{O}[[T]]$ *while* $D_1 f(T,\rho,s) \in \mathfrak{O}[[T]]$ *for arbitrary* ρ.

(ii) *For all integers* $k \geqslant 1$, *we have*

$$D_1^k g(T,\rho,c)|_{T=0} = 12(-1)^{k-1}(k-1)!\,(G_k(\rho,\mathscr{L})Nc - G_k(\rho,c^{-1}\mathscr{L}))$$

and

$$D_1^k f(T,\rho,S)|_{T=0} = 12(-1)^{k-1}(k-1)!\sum_c (G_k(\rho,\mathscr{L})Nc - G_k(\rho,c^{-1}\mathscr{L}))a_c.$$

(iii) *If* $\eta \in \ker[\pi]$ *and* $\rho \notin \mathfrak{p}^{-n}\mathscr{L}$ *then* $g(T +_{\hat{E}} \eta,\rho,c) = g(T,\nu(\eta)+\rho,c)$ *and for all* $\rho \in \mathfrak{g}^{-1}\mathscr{L}$ *we have* $f(T +_{\hat{E}} \eta,\rho,S) = f(T,\nu(\eta)+\rho,S)$.

Proof. — (i) We first show that, if $\alpha \in \mathbf{Q}\mathscr{L}$ and $\alpha \notin \mathfrak{p}^{-n}\mathscr{L}$ for all $n \in \mathbf{Z}_+$, then

$$\wp(\alpha,\mathscr{L}) \quad \text{and} \quad \frac{1}{2}\wp'(\alpha,\mathscr{L}) \in \mathfrak{O}. \tag{16}$$

Indeed if one of $\wp(\alpha)$ and $\frac{1}{2}\wp'(\alpha)$ did not belong to $\mathfrak{O}$, then the equation $\left(\frac{1}{2}\wp'(\alpha)\right)^2 = \wp(\alpha)^3 + a\wp(\alpha) + b$ would imply that the other also didn't, and so $v\left(\frac{1}{2}\wp'(\alpha)^2\right) = v(\wp(\alpha)^3) < 0$. Hence $\dfrac{\wp(\alpha)}{\frac{1}{2}\wp'(\alpha)} \in \mathfrak{m}$ and so α gives rise to a point of $\hat{E}(\mathfrak{m})_{\text{tors}}$ a contradiction.

We divide the proof of (i) proper into three cases (*a*) $\rho \in \mathscr{L}$, (*b*) $\rho \notin \mathscr{L}$ but $\rho \in \mathfrak{p}^{-n}\mathscr{L}$ for some n, and (*c*) $\mathfrak{p} \notin \mathfrak{p}^{-n}\mathscr{L}$ for all n.

(*a*) We may assume that $\rho = 0$. For each c, $\dfrac{\Delta(\mathscr{L})}{\Delta(c^{-1}\mathscr{L})}$ lies in the Hilbert class field of K and has the ideal factorisation c^{-12} (see Lang [17, Chapter 12]). Therefore since E has good reduction at $\mathfrak{p}$ and $\mathfrak{p} \nmid c$, we have $\dfrac{\Delta(\mathscr{L})^{Nc}}{\Delta(c^{-1}\mathscr{L})} = \Delta(\mathscr{L})^{Nc-1}\dfrac{\Delta(\mathscr{L})}{\Delta(c^{-1}\mathscr{L})} \in \bar{\mathbf{Q}} \cap \mathfrak{O}^*$. Recall that there exists

a power series $A(T) \in 1 + \mathfrak{O}[[T]]$ such that

$$x = \frac{1}{T^2} A(T) \quad \text{and} \quad y = -\frac{1}{T^3} A(T), \tag{17}$$

where $T = -\dfrac{x}{y}$ *is a local parameter at the origin of* $\hat{E}$. Hence by Lemma 2 (i)

$$\prod_{\mathfrak{c}} \theta(z, \mathscr{L}; \mathfrak{c}^{-1}\mathscr{L})^{a_{\mathfrak{c}}} = \text{p-unit} \times \prod_{\mathfrak{c}} \left(\prod_{\substack{\gamma \in \mathfrak{c}^{-1}\mathscr{L}/\mathscr{L} \\ \gamma \notin \mathscr{L}}} (\mathscr{P}(z) - \mathscr{P}(\gamma))^{-6} \right)^{a_{\mathfrak{c}}}$$

$$= \text{p-unit} \times \prod_{\mathfrak{c}} \left(\prod_{\gamma}{}' \left(\frac{1}{T^2} A(T) - \mathscr{P}(\gamma) \right)^{-6} \right)^{a_{\mathfrak{c}}}$$

using (17). But for each $\mathfrak{c}$,

$$\prod_{\gamma}{}' \left(\frac{1}{T^2} A(T) - \mathscr{P}(\gamma) \right) \in \frac{1}{T^{2(N\mathfrak{c}-1)}} (1 + T\mathfrak{O}[[T]])$$

by (16) and so $\prod_{\mathfrak{c}} \left(\prod_{\gamma}{}' \left(\frac{1}{T^2} A(T) - \mathscr{P}(\gamma) \right)^{-6} \right)^{a_{\mathfrak{c}}} \in 1 + T\mathfrak{O}[[T]]$ since $\Sigma(N\mathfrak{c} - 1)a_{\mathfrak{c}} = 0$. Applying the operator $D_1 \log_p$ gives rise to an element of $\mathfrak{O}[[T]]$.

(*b*) By case (*a*) $D_1 f(T,0,S) \in \mathfrak{O}[[T]]$ and so $D_1 f(T +_{\hat{E}} \eta, 0, S)$ is well-defined for all $\eta \in \hat{E}(\mathfrak{m})_{\text{tors}}$. Recall that $\prod_{\mathfrak{c}} \theta(z, \mathscr{L}; \mathfrak{c}^{-1}\mathscr{L})^{a_{\mathfrak{c}}}$ is an elliptic function on $\mathscr{L}$ and so may be regarded as a rational function on E which is defined over $\bar{\mathbf{Q}}$. But then $D_1 f(T +_{\hat{E}} \eta, 0, S)$ and $D_1 f(T, \nu(\eta), S)$ can both be interpreted as the Taylor expansion in powers of $T = -\dfrac{\mathscr{P}(z)}{\frac{1}{2}\mathscr{P}'(z)}$ of

$$\frac{d}{dz} \log \prod_{\mathfrak{c}} \theta(z + \nu(\eta), \mathscr{L}, \mathfrak{c}^{-1}\mathscr{L})^{a_{\mathfrak{c}}}$$

and are therefore equal. Hence

$$D_1 f(T, \nu(\eta), S) = D_1 f(T +_{\hat{E}} \eta, 0, S) \in \mathfrak{O}[[T]].$$

(*c*) Again we know that $\dfrac{\Delta(\mathscr{L})^{N\mathfrak{c}}}{\Delta(\mathfrak{c}^{-1}\mathscr{L})}$ is a p-unit and so we need only show that $\theta(\lambda(T) + \rho, \mathscr{L}; \mathfrak{c}^{-1}\mathscr{L})^{-1} \in \mathfrak{O}[[T]]$ with constant term a p-unit,

since we may then again apply $D_1 \log_p$. Now by the addition theorem for $\mathscr{P}(z)$,

$$\mathscr{P}(z+\rho) - \mathscr{P}(\gamma) = \frac{1}{4}\left[\frac{\mathscr{P}'(z) - \mathscr{P}'(\rho)}{\mathscr{P}(z)-\mathscr{P}(\rho)}\right]^2 - \mathscr{P}(z) - \mathscr{P}(\rho) - \mathscr{P}(\gamma)$$

$$= \left[\frac{y-\frac{1}{2}\mathscr{P}'(\rho)}{x-\mathscr{P}(\rho)}\right]^2 - x - \mathscr{P}(\rho) - \mathscr{P}(\gamma)$$

$$= \left[\frac{-T^{-3}A(T)-\frac{1}{2}\mathscr{P}'(\rho)}{T^2A(T)-\mathscr{P}(\rho)}\right]^2 - \frac{1}{T^2}A(T) - \mathscr{P}(\rho) - \mathscr{P}(\gamma).$$

Clearing denominators shows that this power series lies in

$$\mathfrak{O}[\mathscr{P}(\rho), \mathscr{P}'(\rho), \mathscr{P}(\gamma), \mathscr{P}'(\gamma)][[T]] = \mathfrak{O}[[T]]$$

by (16). Hence $\prod_{\gamma} (\mathscr{P}(\gamma(T)+\rho)-\mathscr{P}(\gamma))^6 \in \mathfrak{O}[[T]]$ and since we know that $\theta(\rho, \mathscr{L}; c^{-1}\mathscr{L}) \in \mathfrak{O}^* \cap \bar{\mathbf{Q}}$ (see § 4), the desired property of $g(T,\rho,c)$, and hence also of $f(T,\rho,S)$, follows.

(ii) Since $\frac{1}{\lambda'(T)}\frac{d}{dT} = \frac{d}{dz}$ by the chain rule, this follows at once from the definitions together with Lemma 2 (ii).

(iii) The argument here is similar to that in case (*b*) of (i) (starting with $g(T,\rho,c)$ or $f(T,\rho,S)$ instead of $D_1 f(T,0,S)$) and will be omitted.

This completes the proof of Proposition 4. For $\hat{\rho} \in \mathscr{L}$ we define

$$f_{\hat{\rho}}(T,S) = \sum_{\rho} f(T,\rho,S) <\rho,\hat{\rho}>_{\mathscr{L}} \tag{18}$$

where the sum is taken over a complete set of representatives $\{\rho\}$ of $g^{-1}\mathscr{L}/\mathscr{L}$ in $\mathbf{C}$. This is well-defined since $f(T,\rho,S)$ depends only on ρ modulo $\mathscr{L}$ as observed just before Proposition 4. Let $\tilde{\rho}$ be the image of the complex conjugate of $\Omega^{-1}\hat{\rho}$ in $\mathbf{C}_p$.

PROPOSITION 5. — (i) $f_{\hat{\rho}}(T,S)$ *depends only on* $\hat{\rho}$ *modulo* $\bar{g}\mathscr{L}$.

(ii) $D_1 f_{\hat{\rho}}(T,S) \in \mathfrak{O}[[T]]$.

(iii) *For each* $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$, $(\Delta^{(\beta)} f_{\hat{\rho}}(T,S)) = \omega^{\beta}(\tilde{\rho}) f_{\hat{\rho}}(T,S)$ *whenever* $\hat{\rho} \notin \bar{p}\mathscr{L}$.

$$\text{(iv)}\quad D_1^k f_{\hat\rho}(T,S)|_{T=0} = 12(-1)^{k-1}\mathrm{Ng}\left(\frac{|\Omega|^2\,|d_K|^{\frac12}}{2\pi}\right)^{1-k} \times \sum_{\mathfrak{c}} (G_k(\hat\rho,1,\bar{\mathfrak{g}}\mathscr{L}) - G_k(\mathrm{N}\mathfrak{c}\delta_{\mathfrak{c}}\hat\rho,1,\bar{\mathfrak{g}}\bar{\mathfrak{c}}\mathscr{L}))a_{\mathfrak{c}}\mathrm{N}\mathfrak{c}$$

for all $k \geqslant 1$, *where* $\delta_{\mathfrak{c}}$ *is any integer satisfying* $(\mathrm{N}\mathfrak{c})\delta_{\mathfrak{c}} \equiv 1 \pmod{\mathrm{Ng}}$.

Proof. — (i) It is clearly enough to prove that $\rho \to <\rho,\hat\rho>_{\mathscr{L}}$ depends only on $\hat\rho$ modulo $\bar{\mathfrak{g}}\mathscr{L}$, and for this it suffices to show that $<\rho,\hat\rho>_{\mathscr{L}}=1$ whenever $\hat\rho \in \bar{\mathfrak{g}}\mathscr{L}$. Write $\rho = x\Omega$ with $x \in \mathfrak{g}^{-1}$ and $\hat\rho = \bar a\Omega$ with $a \in \mathfrak{g}$. Then $ax - \bar a\bar x \in 2\mathfrak{O}_K$ and is purely imaginary, and therefore of the form $iy|d_K|^{\frac12}$ with $y \in \mathbf{Z}$. But then $\rho\bar{\hat\rho} - \bar\rho\hat\rho = i|\Omega|^2 y|d_K|^{\frac12}$ and $a(\mathscr{L}) = \frac12|d_K|^{\frac12}|\Omega|^2$ so that $<\rho,\hat\rho>_{\mathscr{L}} = \exp(2\pi i y) = 1$.

(ii) This follows from Proposition 4 (i) since $<\rho,\hat\rho>_{\mathscr{L}}$ is a root of unity.

(iii) If $a \in \mathfrak{O}_{K_\mathfrak{p}}$ define $F_{a,\hat\rho}(T,S) = \sum_{\eta \in \ker[\pi]} f_{\hat\rho}(T +_{\mathfrak{E}} \eta, S)t_a(\eta)$.

Using (4) we have

$$(\Delta^{(\beta)}F_{a,\hat\rho})(T,S) = \omega^\beta(a)F_{a,\hat\rho}(T,S), \quad \text{if} \quad a \in \mathfrak{O}_{K_\mathfrak{p}}^*$$
$$= 0 \quad \text{if} \quad a \equiv 0 \pmod{\mathfrak{m}_{K_\mathfrak{p}}}.$$

But

$$\sum_\eta f_{\hat\rho}(T +_{\mathfrak{E}} \eta, S)t_a(\eta) = \sum_{\eta,\rho} f(T +_{\mathfrak{E}} \eta, \rho, S)t_a(\eta)\langle\rho,\hat\rho\rangle_{\mathscr{L}}$$
$$= \sum_{\eta,\rho} f(T, \nu(\eta)+\rho, S)t_a(\eta)\langle\rho+\nu(\eta),\hat\rho\rangle_{\mathscr{L}}\langle-\nu(\eta),\hat\rho\rangle_{\mathscr{L}}$$

(by Proposition 4 (iii))

$$= \sum_\rho f(T,\rho,S)\langle\rho,\hat\rho\rangle_{\mathscr{L}} \sum_\eta t_a(\eta)\langle-\nu(\eta),\hat\rho\rangle_{\mathscr{L}}$$
$$= f_{\hat\rho}(T,S)\sum_\eta t_a(\eta)\langle-\nu(\eta),\hat\rho\rangle_{\mathscr{L}}.$$

Now $\eta \mapsto t_a(\eta)$ and $\eta \mapsto \langle-\nu(\eta),\hat\rho\rangle_{\mathscr{L}}$ both give rise to additive characters on $E_\mathfrak{p}(\mathbf{C})$ and hence $\sum_\eta t_a(\eta)\langle-\nu(\eta),\hat\rho\rangle_{\mathscr{L}} = 0$ except when a belongs to the unique residue class (mod $\mathfrak{p}$) such that $t_a(\eta) = \langle\nu(\eta),\hat\rho\rangle_{\mathscr{L}}$, in which case the sum is q. Therefore $(\Delta^{(\beta)}f_{\hat\rho})(T,S) = \omega^\beta(a)f_{\hat\rho}(T,S)$ for this a, provided $a \in \mathfrak{O}_{K_\mathfrak{p}}^*$. Since we have agreed that $\langle\nu(\eta),\Omega\rangle_{\mathscr{L}} = t_1(\eta)$

we find that $t_a([a](\eta))\langle av(\eta),\Omega\rangle_{\mathscr{L}} = \langle v(\eta),\Omega\bar{a}\rangle_{\mathscr{L}}$ and so $a \equiv \overline{\Omega^{-1}\hat{\rho}} \pmod{\mathfrak{p}}$ whence indeed $a \in \mathfrak{O}_{K_\mathfrak{p}}^*$ and $\omega^\beta(a) = \omega^\beta(\tilde{\rho})$. This proves (iii).

(iv) By Proposition 4 (ii)

$$D_1^k f_{\hat{\rho}}(T,S)|_{T=0} = 12(-1)^{k-1}(k-1)! \sum_{\mathfrak{c}}\sum_{\rho}(G_k(\rho,\mathscr{L})N\mathfrak{c} - G_k(\rho,\mathfrak{c}^{-1}\mathscr{L}))\langle\rho,\hat{\rho}\rangle_{\mathscr{L}}^{a_\mathfrak{c}}$$

whenever $k \geqslant 1$. By the functional equation Lemma 3 (with $\Lambda = \mathscr{L}$, $\Lambda' = \mathfrak{g}^{-1}\mathscr{L}$ so that $\Lambda'' = \bar{\mathfrak{g}}\mathscr{L}$, $a(\Lambda) = \frac{1}{2}|\Omega|^2|d_K|^{\frac{1}{2}}$, $(\Lambda' : \Lambda) = N\mathfrak{g}$, and $s = k$), we obtain

$$12(k-1)!(-1)^{k-1}\sum_{\rho} G_k(\rho,\mathscr{L})\langle\rho,\hat{\rho}\rangle_{\mathscr{L}} = 12(-1)^{k-1}N\mathfrak{g}\left(\frac{|\Omega|^2|d_K|^{\frac{1}{2}}}{2\pi}\right)^{1-k} G_k(\hat{\rho},1,\bar{\mathfrak{g}}\mathscr{L}).$$

On the other hand, if $\rho \in \mathfrak{g}^{-1}\mathscr{L}$ and $\hat{\rho} \in \mathscr{L}$, then $\langle\rho,\hat{\rho}\rangle_{\mathfrak{c}^{-1}\mathscr{L}} = \langle\rho,\hat{\rho}\rangle_{\mathscr{L}}^{N\mathfrak{c}}$ is a $N\mathfrak{g}-$th root of unity, so that if $\delta_\mathfrak{c}$ is an integer with $N\mathfrak{c}\,\delta_\mathfrak{c} \equiv 1 \pmod{N\mathfrak{g}}$ we find $\langle\rho,\hat{\rho}\rangle_{\mathscr{L}} = \langle\rho,\hat{\rho}\rangle_{\mathfrak{c}^{-1}\mathscr{L}}^{\delta_\mathfrak{c}} = \langle\rho,\delta_\mathfrak{c}\hat{\rho}\rangle_{\mathfrak{c}^{-1}\mathscr{L}}$. Applying the functional equation with $\Lambda = \mathfrak{c}^{-1}\mathscr{L}$, $\Lambda' = \mathfrak{g}^{-1}\mathfrak{c}^{-1}\mathscr{L}$, etc... we obtain

$$12(k-1)!(-1)^{k-1}\sum_{\rho} G_k(\rho,\mathfrak{c}^{-1}\mathscr{L})\langle\rho,\hat{\rho}\rangle_{\mathscr{L}} = 12(-1)^{k-1}N\mathfrak{g}\left(\frac{|\Omega|^2|d_K|^{\frac{1}{2}}}{2\pi N\mathfrak{c}}\right)^{1-k} G_k(\delta_\mathfrak{c}\hat{\rho},1,\mathfrak{c}^{-1}\bar{\mathfrak{g}}\mathscr{L}).$$

But $G_k(\delta_\mathfrak{c}\hat{\rho},1,\mathfrak{c}^{-1}\bar{\mathfrak{g}}\mathscr{L}) = N\mathfrak{c}^{2-k}G_k(N\mathfrak{c}\delta_\mathfrak{c}\hat{\rho},1,\bar{\mathfrak{c}}\bar{\mathfrak{g}}\mathscr{L})$, hence, simplifying and summing over $\mathfrak{c}$ we obtain (iv).

Proof of Theorem A. — We use the notation and hypothesis of Theorem A : in particular a is an element of $\mathfrak{O}_K$ which is not divisible by $\mathfrak{p}$. Then $\hat{\rho} = \Omega\bar{a}$ and so $\tilde{\rho} = a$. Applying Theorem 1 with $f(T) = f_{\hat{\rho}}(T,S)$ and $\alpha = 0$, we deduce the existence of a locally analytic function $G_\mathfrak{p}(a,s,\mathfrak{g},S) : \mathbf{Z}_p \to \mathbf{C}_p$ satisfying

$$G_\mathfrak{p}(a,0,\mathfrak{g},S) = f_{\hat{\rho}}(0,S) \tag{19}$$

and

$$(20)\quad G_p(a,k,\mathfrak{g},S) = -12\frac{N\mathfrak{g}}{\Omega_p^k}\left[\frac{|\Omega|^2|d_K|^{\frac{1}{2}}}{2\pi}\right]^{1-k}\omega^{-\beta}(\tilde{\mathfrak{p}})$$
$$\times\sum_{\mathfrak{c}}(G_k(\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\mathscr{L})-G_k(N\mathfrak{c}\delta_{\mathfrak{c}}\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\bar{\mathfrak{c}}\mathscr{L}))N\mathfrak{c}a_{\mathfrak{c}}$$

for every integer $k \geqslant 1$.

We now suppose that the $\mathfrak{c}$'s each have a generator $\gamma_{\mathfrak{c}} \equiv 1 \pmod{\mathfrak{g}}$. In this case

$$G_k(N\mathfrak{c}\delta_{\mathfrak{c}}\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\bar{\mathfrak{c}}\mathscr{L}) = G_k(\gamma_{\mathfrak{c}}\bar{\gamma}_{\mathfrak{c}}\delta_{\mathfrak{c}}\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\bar{\mathfrak{c}}\mathscr{L})$$
$$= \frac{\gamma_{\mathfrak{c}}^k}{N\mathfrak{c}}G_k(\gamma_{\mathfrak{c}}\delta_{\mathfrak{c}}\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\mathscr{L}) = \frac{\gamma_{\mathfrak{c}}^k}{N\mathfrak{c}}G_k(\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\mathscr{L})$$

since $\delta_{\mathfrak{c}}\gamma_{\mathfrak{c}} - 1 \in \mathfrak{g}$. Hence the above formula reduces to

$$G_p(a,k,\mathfrak{g},S) = -12\frac{N\mathfrak{g}}{\Omega_p^k}\left[\frac{|\Omega|^2|d_K|^{\frac{1}{2}}}{2\pi}\right]^{1-k}\omega^{-\beta}(\tilde{\mathfrak{p}})$$
$$\times G_k(\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\mathscr{L})\sum_{\mathfrak{c}}(N\mathfrak{c}-\gamma_{\mathfrak{c}}^k)a_{\mathfrak{c}}.$$

Since $\gamma_{\mathfrak{c}} \equiv 1 \pmod{\mathfrak{g}}$ and $\mathfrak{p}\,|\,\mathfrak{g}$ the function

$$C_0(s) = \sum_{\mathfrak{c}}(N\mathfrak{c}-\gamma_{\mathfrak{c}}^s)a_{\mathfrak{c}}$$

is well-defined on $\mathbf{Z}_p$, and if $\tilde{\mathfrak{p}} = a \in \mathfrak{O}_K$ then

$$G_k(\hat{\mathfrak{p}},1,\bar{\mathfrak{g}}\mathscr{L}) = \frac{\bar{\Omega}^k}{|\Omega|^2}G_k(\bar{a},1,\bar{\mathfrak{g}}).$$

Hence if we define

$$G_p(a,s,\mathfrak{g}) = \frac{G_p(a,s,\mathfrak{g},S)}{12N\mathfrak{g}C_0(s)}$$

we find that

$$G_p(a,k,\mathfrak{g}) = \frac{1}{\Omega_p^k}\left[\left(\frac{|d_K|^{\frac{1}{2}}}{2\pi}\right)^{1-k}\frac{1}{\Omega^k}\omega^{-\beta}(a)G_k(\bar{a},1,\bar{\mathfrak{g}})\right]$$

for all $k \geqslant 1$, which shows that $G_p(a,s,\mathfrak{g})$ is independent of the choice of S as our notation suggests. It remains to prove that $G_p(a,s,\mathfrak{g})$ has a simple pole at $s = 0$ with residue $(N\mathfrak{g})^{-1}$. Clearly

$C_0(s) = -\sum_{\mathfrak{c}} (\log_p \gamma_{\mathfrak{c}}) a_{\mathfrak{c}} s + O(s^2)$. If we make the additional hypothesis that the $\mathfrak{c}$'s are mutually coprime then $\sum_{\mathfrak{c}} (\log_p \gamma_{\mathfrak{c}}) a_{\mathfrak{c}} \neq 0$ and so it suffices to show that $G_p(\mathfrak{a},0,\mathfrak{g},S) = -12 \sum_{\mathfrak{c}} (\log_p \gamma_{\mathfrak{c}}) a_{\mathfrak{c}}$. Now

$$G_p(\mathfrak{a},0,\mathfrak{g},S) = f_{\hat{\rho}}(0,S) = f(0,0,S) + \sum_{\rho \neq 0} f(0,\rho,S) \langle \rho, \hat{\rho} \rangle_{\mathscr{L}}$$

so that we need only show that $f(0,0,S) = -12 \sum_{\mathfrak{c}} (\log_p \gamma_{\mathfrak{c}}) a_{\mathfrak{c}}$ and $f(0,\rho,S) = 0$ for the other ρ. Indeed (cf. the proof of case (*a*) of Proposition 4 (ii)), we have

$$f(0,0,S) = \log_p \prod_{\mathfrak{c}} \left(\frac{\Delta(\mathscr{L})^{N\mathfrak{c}}}{\Delta(\mathfrak{c}^{-1}\mathscr{L})} \right)^{a_{\mathfrak{c}}}$$

$$= \log_p \left(\Delta(\mathscr{L})^{\sum_{\mathfrak{c}} (N\mathfrak{c}-1)a_{\mathfrak{c}}} \prod_{\mathfrak{c}} \gamma_{\mathfrak{c}}^{-12a_{\mathfrak{c}}} \right) = -12 \sum_{\mathfrak{c}} (\log_p \gamma_{\mathfrak{c}}) a_{\mathfrak{c}}.$$

On the other hand the case $\rho \neq 0$ will be dealt with if we can show that $\prod_{\mathfrak{c}} \theta(\rho, \mathscr{L}; \mathfrak{c}^{-1}\mathscr{L})^{a_{\mathfrak{c}}}$ is a root of unity. It follows easily from (5), (10) and (11) that $\theta(z,\Lambda)$ satisfies the identity

$$\theta(z+w,\Lambda) = \theta(z,\Lambda) \times \exp\left(\frac{6\pi}{a(\Lambda)} w(w+2z) \right)$$

for $z \in \mathbf{C}$ and $w \in \Lambda$, and so

$$\theta(\rho,\mathfrak{c}^{-1}\mathscr{L}) = \theta(\gamma_{\mathfrak{c}}\rho,\mathscr{L}) = \theta(\rho + (\gamma_{\mathfrak{c}}-1)\rho,\mathscr{L})$$

$$= \theta(\rho,\mathscr{L}) \exp\left\{ \frac{12\pi}{|\Omega|^2 |d_K|^{\frac{1}{2}}} (\gamma_{\mathfrak{c}}-1)(\gamma_{\mathfrak{c}}+1)\rho\bar{\rho} \right\}.$$

The proof will be complete once it is shown that

$$\frac{12\pi\rho\bar{\rho}}{|\Omega|^2 |d_K|^{\frac{1}{2}}} \sum_{\mathfrak{c}} (\bar{\gamma}_{\mathfrak{c}}-1)(\gamma_{\mathfrak{c}}+1)a_{\mathfrak{c}} \in i\pi\mathbf{Q}$$

and this follows almost at once from the facts $\frac{\rho\bar{\rho}}{|\Omega|^2} \in \mathbf{Q}$, $\gamma_{\mathfrak{c}}\bar{\gamma}_{\mathfrak{c}} = N\mathfrak{c}$ and $\sum_{\mathfrak{c}} (N\mathfrak{c}-1)a_{\mathfrak{c}} = 0$.

3. p-adic L-Functions of Elliptic Curves.

We now begin the task of associating p-adic L-functions to elliptic curves with complex multiplication. We keep the notation already introduced. In particular E is an elliptic curve satisfying conditions (i) to (iii) of the Introduction and F is an abelian extension of K. If L is an algebraic number field, we write J_L for the idele group of L, while if L′ is a subfield of L, q a prime of L′ and $\underset{\sim}{A} \in J_L$, then A_q denotes the direct product of the components of $\underset{\sim}{A}$ at the primes of L above q. If $\underset{\sim}{A} \in J_L$, we write $\iota(\underset{\sim}{A})$ for the ideal $\prod_{\mathfrak{D}} \mathfrak{D}^{\mathrm{ord}_{\mathfrak{D}} A_{\mathfrak{D}}}$ of L where the product is over all the primes of L. We shall write $N_{L/L'}$ for the norm map from L to L′ (on elements, ideals, ideles or components of ideles above a given prime of L′). On the other hand if $\mathfrak{G}$ is an integral ideal of L, then $I(\mathfrak{G})$ denotes the group of fractional ideals of L prime to $\mathfrak{G}$, $P(\mathfrak{G})$ the subgroup of $I(\mathfrak{G})$ consisting of principal ideals, and $P_{\mathfrak{G}} = \{\mathscr{A} \in P(\mathfrak{G}) \mid \mathscr{A}$ has a generator A with $A \equiv 1 \pmod^{\times} \mathfrak{G}\}$. Finally we write $\Gamma(\mathfrak{G})$ for the ray class group $I(\mathfrak{G})/P_{\mathfrak{G}}$, while the image of $\mathscr{C} \in I(\mathfrak{G})$ in $\Gamma(\mathfrak{G})$ is denoted by $\mathrm{Cl}_{\mathfrak{G}}(\mathscr{C})$.

Fix an integral ideal $\mathfrak{f}$ of K and let $\lambda: I(\mathfrak{f}) \to \bar{\mathbf{Q}}^*$ be a homomorphism satisfying the following conditions:

(i) If $\mathfrak{a} \in P_{\mathfrak{f}}$ with generator $a \equiv 1 \pmod^{\times} \mathfrak{f}$, then $\lambda(\mathfrak{a}) = a$,

(ii) $\lambda(\mathfrak{a}) \equiv 1 \pmod{\mathfrak{m}}$ for all $\mathfrak{a} \in I(\mathfrak{f})$ (recall that $\mathfrak{m}$ is the maximal ideal of $\mathfrak{O}$ and we have fixed embedding $\bar{\mathbf{Q}} \subset\!\!\rightarrow \mathbf{C}_p$).

Condition (ii) clearly implies that $\mathfrak{p} \mid \mathfrak{f}$. If $\mathfrak{g}$ is an ideal of K divisible by $\mathfrak{f}$, and $C \in \Gamma(\mathfrak{g})$, and k an integer $\geqslant 1$, define

$$\zeta_\infty(s,k,\mathfrak{g},C) = \sum_{\mathfrak{a} \in C} \frac{\lambda(\mathfrak{a})^k}{N\mathfrak{a}^s}$$

where the sum is taken over all integral ideals $\mathfrak{a}$ of K belonging to C. Suppose that $\mathfrak{a}_c$ is an integral ideal belonging to C^{-1}. Since $\mathfrak{p} \mid \mathfrak{f}$ and $N\mathfrak{p} \geqslant 5$, every ideal $\mathfrak{a}_c\mathfrak{a}$ with $\mathfrak{a} \in C$ has a unique generator $a \equiv 1 \pmod{\mathfrak{g}}$ and $a \equiv 0 \pmod{\mathfrak{a}_c}$; conversely as a runs through all the solutions of these congruences, so $(a)\mathfrak{a}_c^{-1}$ runs through all the integral ideals belonging to C. Hence

$$\sum_{\mathfrak{a} \in C} \frac{\lambda(\mathfrak{a})^k}{N\mathfrak{a}^s} = \frac{N\mathfrak{a}_c^s}{\lambda(\mathfrak{a}_c)^k} \sum_a \frac{\lambda((a))^k}{N(a)^s} = \frac{N\mathfrak{a}_c^s}{\lambda(\mathfrak{a}_c)^k} \sum_a \frac{a^k}{Na^s},$$

where the summation in the last two sums is over all a such that $a \equiv 1 \pmod{\mathfrak{g}}$ and $a \equiv 0 \pmod{\mathfrak{a}_c}$. Fixing once and for all a solution a_c of $a \equiv 1 \pmod{\mathfrak{g}}$ and $a \equiv 0 \pmod{\mathfrak{a}_c}$ we see that

$$\zeta_\infty(s,k,\mathfrak{g},C) = \frac{N\mathfrak{a}_c^s}{\lambda(\mathfrak{a}_c)^k} G_k(\bar{a}_c,s,\bar{\mathfrak{a}}_c\bar{\mathfrak{g}}).$$

This shows that $\zeta_\infty(s,k,\mathfrak{g},C)$ has an analytic continuation to the whole complex plane; in particular we write $\zeta_\infty(k,\mathfrak{g},C)$ for $\zeta_\infty(1,k,\mathfrak{g},C)$ so that

$$\zeta_\infty(k,\mathfrak{g},C) = \frac{N\mathfrak{a}_c}{\lambda(\mathfrak{a}_c)^k} G_k(\bar{a}_c,1,\bar{\mathfrak{a}}_c\bar{\mathfrak{g}}).$$

On the other hand we define the $\mathfrak{p}$-adic function $\zeta_\mathfrak{p}(s,\mathfrak{g},C)$ by

$$\zeta_\mathfrak{p}(s,\mathfrak{g},C) = \frac{N\mathfrak{a}_c}{\lambda(\mathfrak{a}_c)^s} G_\mathfrak{p}(a_c,s,\mathfrak{a}_c\mathfrak{g})$$

for $s \in \mathbf{Z}_p$. Note that $\lambda(\mathfrak{a}_c)^s$ is well-defined since $\lambda(\mathfrak{a}_c) \equiv 1 \pmod{\mathfrak{m}}$. One sees at once that $\zeta_\mathfrak{p}(s,\mathfrak{g},C)$ does not depend on the choice of $\mathfrak{a}_c$ and a_c: moreover Theorem A implies that $s \mapsto \zeta_\mathfrak{p}(s,\mathfrak{g},C)$ is a locally meromorphic function which is analytic except for a simple pole at $s = 0$ with residue $(N\mathfrak{g})^{-1}$ while if $k \geqslant 1$ is an integer, then

$$\zeta_\mathfrak{p}(k,\mathfrak{g},C) = \frac{1}{\Omega_\mathfrak{p}^k}\left[\left(\frac{|d_K|^{\frac{1}{2}}}{2\pi}\right)^{1-k} \frac{\zeta_\infty(k,\mathfrak{g},C)}{\Omega^k}\right], \tag{21}$$

(the factor $\omega^{-k}(a_c)$ being 1 since $a_c \equiv 1 \pmod{\mathfrak{p}}$).

Now let $\chi : \mathrm{Gal}(K^{ab}/K) \to \bar{\mathbf{Q}}$ be a character of finite order, which can be viewed as a character of J_K, and if $\mathfrak{h}$ is any multiple of the conductor of χ, we obtain a character of $I(\mathfrak{h})$ in the usual manner. Let $\mathfrak{g}$ be the least common multiple of $\mathfrak{f}$ and the conductor of χ, and define

$$L_\infty^*(s,k,\chi) = \prod_\mathfrak{g}\left(1 - \frac{\lambda(\mathfrak{q})^k\chi(\mathfrak{q})}{N\mathfrak{q}^s}\right)^{-1} = \sum_{C \in \Gamma(\mathfrak{g})} \zeta_\infty(s,k,\mathfrak{g},C)\chi(C)$$

where the product in the middle is taken over all primes $\mathfrak{q}$ of K prime to $\mathfrak{g}$. We use the asterisk to indicate that this is not necessarily a primitive L-function owing to the possible existence of primes dividing $\mathfrak{g}$ at which $\lambda^k\chi$ is unramified. Again L_∞ has an analytic continuation to the whole complex plane and we can consider its value $L_\infty(1,k,\chi)$. On the other

hand we define the p-adic L−function $L_p(s,\chi)$ by

$$L_p(s,\chi) = \sum_{C \in \Gamma(\mathfrak{g})} \zeta_p(s,\mathfrak{g},C)\chi(C). \tag{22}$$

We then have

THEOREM 6. — *$L_p(s,\chi)$ is a locally meromorphic function on $\mathbf{Z}_p$ which is locally analytic except when χ is trivial in which case the only singularity is a simple pole at $s = 0$ with residue*

$$\frac{h_K}{m_K} \prod_{\mathfrak{l}} \left(1 - \frac{1}{N\mathfrak{l}}\right)^{-1},$$

h_K being the class number and m_K the number of roots of unity of K, and the product is taken over all primes $\mathfrak{l}$ of K which divide $\mathfrak{f}$. Moreover

$$L_p(k,\chi) = \frac{1}{\Omega_p^k}\left[\left(\frac{|d_K|^{\frac{1}{2}}}{2\pi}\right)^{1-k} \frac{L_\infty^*(1,k,\chi)}{\Omega^k}\right] \tag{23}$$

for $k \in \mathbf{Z}$ with $k \geqslant 1$.

Proof. — If χ is trivial $\mathfrak{g} = \mathfrak{f}$ and the residue at $s = 0$ is $\frac{1}{N\mathfrak{g}} \times |\Gamma(\mathfrak{g})|$ which is equal to the asserted formula. The other assertions follow at once from the previous remarks.

The discussion below leads to a specific choice of λ in Theorem 6 from which the p-adic L-functions of E are obtained. Let M be a finite extension of K and $\varphi : J_M \to \bar{\mathbf{Q}}^*$ a homomorphism satisfying:

(*a*) ker φ is an open subgroup of J_M.

(*b*) There exists an integral ideal $\mathfrak{G}$ of M such that ker φ contains the subgroup $\prod_{\mathfrak{P}} (1 + \mathfrak{G}\mathfrak{O}_{M_\mathfrak{P}})^\times$ of J_M, where the product is taken over all the primes $\mathfrak{P}$ of M and $(1+\mathfrak{G}\mathfrak{O}_{M_\mathfrak{P}})^\times$ is interpreted as $\mathfrak{O}^*_{M_\mathfrak{P}}$ if $\mathfrak{P} \nmid \mathfrak{G}$. The smallest such $\mathfrak{G}$ is called the conductor of φ.

(*c*) If $\underset{\sim}{A} \in J_M$ satisfies $A_\mathfrak{P} = 1$ for all $\mathfrak{P} | \mathfrak{G}$ and $\iota(\underset{\sim}{A}) \in P_\mathfrak{G}$ with generator A, then $\varphi(\underset{\sim}{A}) = N_{M/K}A$.

(*d*) If $\underset{\sim}{A} = (\ldots, A, A, \ldots)$ with $A \in M^*$, then $\varphi(\underset{\sim}{A}) = N_{M/K}A$.

Associated to such a φ, there is a p-adic character $\varphi_p : J_M \to \mathbf{C}_p^*$ defined by

$$\varphi_p(\underset{\sim}{A}) = \varphi(\underset{\sim}{A})(N_{M/K}A_p)^{-1}. \tag{24}$$

LEMMA 7. — (i) $\varphi_\mathfrak{p}$ *is continuous (with regard to the topology of* $\mathbf{C}_p$*), comes from a character of* $\mathrm{Gal}(M^{ab}/M)$ *(of infinite order), and its image is a compact subgroup of* $\mathfrak{O}^*$.

(ii) *If* $\varphi' : J_M \to \bar{\mathbf{Q}}^*$ *is another homomorphism satisfying (a) to (d), then* $\varphi\varphi'^{-1} = \varphi_\mathfrak{p}\varphi'^{-1}_\mathfrak{p}$ *comes from a character of finite order of* $\mathrm{Gal}(M^{ab}/M)$.

(iii) *There is at most one such* φ *(for fixed* M *and* $\mathfrak{p}$*) having the additional property that* $\varphi_\mathfrak{p}$ *takes values in* $(1+\mathfrak{p}\mathfrak{O}_{K_\mathfrak{p}})^\times$.

Proof. — (i) (*a*) implies that φ is continuous. On the other hand $\underset{\sim}{A} \mapsto (N_{M/K}A_\mathfrak{p})^{-1}$ is certainly continuous, hence the continuity of $\varphi_\mathfrak{p}$. Since $\mathbf{C}_p$ is totally disconnected, $\ker \varphi_\mathfrak{p}$ contains the connected component of the identity of J_M, whence $\varphi_\mathfrak{p}$ comes from a character of $\mathrm{Gal}(M^{ab}/M)$. Since $\mathrm{Gal}(M^{ab}/M)$ is compact, im $\varphi_\mathfrak{p}$ is compact and in particular contained in $\mathfrak{O}^*$.

(ii) Clearly $\varphi\varphi'^{-1} = \varphi_\mathfrak{p}\varphi'^{-1}_\mathfrak{p}$. If $\mathfrak{G}$ and $\mathfrak{G}'$ are the conductor of φ and φ', then (*b*), (*c*) and (*d*) imply that $\varphi\varphi'^{-1}$ is trivial on a subgroup of finite index of J_M, and (i) then shows that $\ker(\varphi_\mathfrak{p}\varphi'^{-1}_\mathfrak{p})$ corresponds to an extension of M of conductor dividing $\mathfrak{G}\mathfrak{G}'$, i.e. a finite abelian extension of M.

(iii) If φ and φ' are such that $\varphi_\mathfrak{p}$ and $\varphi'_\mathfrak{p}$ take values in $(1+\mathfrak{p}\mathfrak{O}_{K_\mathfrak{p}})^\times$, then by (i) $\varphi\varphi'^{-1}$ is a character of finite order taking values in $(1+\mathfrak{p}\mathfrak{O}_{K_\mathfrak{p}})^\times$. Since $N\mathfrak{p} \geqslant 5$, this implies that $\varphi' = \varphi$.

Now let $\psi : J_F \to K^*$ be the Hecke character of E over F as in Serre-Tate [26, Theorem 10]. In fact ψ is a homomorphism satisfying the properties (*a*) to (*d*) above. Let $\varepsilon : \mathrm{Gal}(\bar{\mathbf{Q}}/F) \to K_\mathfrak{p}^*$ be the character giving the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/F)$ on the $\mathfrak{p}$-division points of E. It is clear that ε factors through to a character of $\mathrm{Gal}(F(E_\mathfrak{p})/F)$, and class field theory enables us to view it as a character of J_F. Since ε is of finite order, $\psi\varepsilon^{-1}$ is also a homomorphism satisfying (*a*) to (*d*). Let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_r$ be the primes of F above $\mathfrak{p}$.

PROPOSITION 8. —

(i) *The conductor of* $\psi\varepsilon^{-1}$ *is* (1) *or* $\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_r$ *according as to whether* $F(E_\mathfrak{p}) = F$ *or not, and* $(\psi\varepsilon^{-1})_\mathfrak{p}$ *takes values in* $(1+\mathfrak{p}\mathfrak{O}_{K_\mathfrak{p}})^\times$.

(ii) *There exists a homomorphism* $\lambda : J_K \to \bar{\mathbf{Q}}^*$ *satisfying (a) to (d) above as well as the following:*

(*e*) *The conductor of* λ *is* $\mathfrak{p}$.

(*f*) $\lambda_{\mathfrak{p}}(\underset{\sim}{a}) \equiv 1 \pmod{\mathfrak{m}}$ *for all* $\underset{\sim}{a} \in J_K$.

(*g*) $(\psi\varepsilon^{-1})(\underset{\sim}{A}) = \lambda(N_{F/K}\underset{\sim}{A})$ *for all* $\underset{\sim}{A} \in J_F$.

Proof. — (i) We first show that $\psi\varepsilon^{-1}$ is unramified at all primes of F that do not lie above $\mathfrak{p}$. Let $\mathfrak{Q}$ be such a prime, and regard the local units $\mathfrak{O}_{F_\mathfrak{Q}}^*$ as being embedded in J_F. Now $\psi(\underset{\sim}{A})P = \varepsilon(\underset{\sim}{A})P$ for all $\underset{\sim}{A} \in \mathfrak{O}_{F_\mathfrak{Q}}^*$ and $P \in E_\mathfrak{p}$, and so $\psi(\underset{\sim}{A}) \equiv \varepsilon(\underset{\sim}{A}) \pmod{\mathfrak{p}}$ and $(\psi\varepsilon^{-1})(\underset{\sim}{A}) \equiv 1 \pmod{\mathfrak{p}}$. On the other hand ψ and ε are both of finite order when restricted to $\mathfrak{O}_{F_\mathfrak{Q}}^*$, and so if $\psi\varepsilon^{-1}$ were ramified at $\mathfrak{Q}$ we could choose $\underset{\sim}{A}$ so that $\psi\varepsilon^{-1}(\underset{\sim}{A})$ were a primitive p-th root of unity. But $\psi\varepsilon^{-1}$ takes values in $K_\mathfrak{p}^*$ and $\mu_p \not\subseteq K$ since $p \geqslant 5$. Hence $\psi\varepsilon^{-1}$ is unramified at $\mathfrak{Q}$. The fact that $F(E_{\text{tors}})$ is abelian over K implies that the conductor of $\psi\varepsilon^{-1}$ is invariant under Gal (F/K) and is therefore of the form $(\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_r)^e$ for some $e \geqslant 0$. Since E has good reduction at each prime of F above $\mathfrak{p}$, ψ is unramified at $\mathfrak{p}$ and so the conductor of $\psi\varepsilon^{-1}$ is the same as the $\mathfrak{p}$-part of the conductor of ε. On the other hand the fact that $\hat{E}$ is isomorphic to a Lubin-Tate group implies that $[F(E_\mathfrak{p}) : F]$ divides $q - 1$, and so the ramification must be tame, i.e. $e \leqslant 1$. But then clearly $e = 0$ if and only if ε is trivial, that is if and only if $F(E_\mathfrak{p}) = F$.

Finally we show that $(\psi\varepsilon^{-1})_\mathfrak{p}$ takes values in $(1 + \mathfrak{p}\mathfrak{O}_{K_\mathfrak{p}})^\times$. Since $(1 + \mathfrak{p}\mathfrak{O}_{K_\mathfrak{p}})^\times$ is an open subgroup of $\mathfrak{O}_{K_\mathfrak{p}}^*$ its preimage is an open subgroup of J_F. Now we have already seen that $(\psi\varepsilon^{-1})_\mathfrak{p}(\underset{\sim}{A}) \in (1 + \mathfrak{p}\mathfrak{O}_{K_\mathfrak{p}})^\times$ if $A_\mathfrak{p} = 1$, and so this must hold under the weaker assumption $A_\mathfrak{p} \equiv 1 \pmod{\mathfrak{p}^r}$ for some $r \geqslant 0$. The fact that it holds in general now follows from the approximation theorem, together with the fact that $(\psi\varepsilon^{-1})_\mathfrak{p}(\underset{\sim}{A}) = 1$ if $\underset{\sim}{A} = (\ldots A, A, \ldots)$ with $A \in F^*$.

(ii) We define λ as follows : suppose in the first place that $\underset{\sim}{a} \in J_K$ with $a_\mathfrak{p} = 1$, and that the ideal $\imath(\underset{\sim}{a})$ is principal with generator a a unit at $\mathfrak{p}$. We then define $\lambda(\underset{\sim}{a})$ to be $\omega^{-1}(a)a$. Let C be the ideal class group of K, and $C = C_1 \times C_2 \times \cdots \times C_r$ a decomposition of C into cyclic subgroups C_i. For each i, let m_i be the order of C_i and $\underset{\sim}{a}_i \in J_K$ an idele with $a_{i,\mathfrak{p}} = 1$ such that the class of $\imath(\underset{\sim}{a}_i)$ generates C_1. We then define $\lambda(\underset{\sim}{a}_i)$ to be $(\lambda(\underset{\sim}{a}_i^{m_i}))^{1/m_i}$, where we have fixed once and for all an m_i-th root of $\lambda(\underset{\sim}{a}_i^{m_i})$ which is congruent to 1 modulo $\mathfrak{m}$. Then if $\underset{\sim}{a} \in J_K$ has $a_\mathfrak{p} = 1$ there exist unique ℓ_i with $0 \leqslant \ell_i < m_i$ and $\underset{\sim}{b}$ will $b_\mathfrak{p} = 1$ and $\imath(\underset{\sim}{b})$ principal such that $\underset{\sim}{a} = \left(\prod_{i=1}^{r} \underset{\sim}{a}_i^{\ell_i}\right)\underset{\sim}{b}$; we define $\lambda\left(\underset{\sim}{a}\prod_{i=1}^{r} \lambda(\underset{\sim}{a}_i)^{\ell_i}\right)\lambda(\underset{\sim}{b})$.

If $\underset{\sim}{a} = (\ldots a,a,\ldots)$ with $a \in K^*$ we define $\lambda(\underset{\sim}{a}) = a$. We thus obtain a homomorphism $K^*J_{K,\mathfrak{p}} \to \bar{\mathbf{Q}}$, where $J_{K,\mathfrak{p}}$ denotes the subgroup of $\underset{\sim}{a} \in J_K$ with $a_{\mathfrak{p}} = 1$. It is easily seen from the definitions that this homomorphism is continuous, and that in fact its kernel is an open subgroup of $K^*J_{K,\mathfrak{p}}$. Since $K^*J_{K,\mathfrak{p}}$ is dense in J_K we can extend λ by continuity to J_K, and it satisfies (a).

We now show that λ satisfies the conditions (b) to (g). It is clear that the restriction to $\mathfrak{O}_{K_{\mathfrak{q}}}^*$ is trivial for all primes $\mathfrak{q} \neq \mathfrak{p}$ of K. On the other hand the restriction of λ to $(1+\mathfrak{p}\mathfrak{O}_{K_{\mathfrak{p}}})^\times$ is trivial since K does not contain any p-power roots of unity; to see that λ is non-trivial on the whole of $\mathfrak{O}_{K_{\mathfrak{p}}}^*$ we observe that $\lambda(\underset{\sim}{u}) = -1$, where $\underset{\sim}{u}$ is the idele with $u_{\mathfrak{p}} = -1$ and all other components one. This proves (b) and (e). (c) follows since if $\underset{\sim}{a} \in J_K$ has $a_{\mathfrak{p}} = 1$ and $\iota(\underset{\sim}{a})$ has a generator $a \equiv 1 \pmod{\mathfrak{p}}$ then $\omega^{-1}(a) = 1$, while (d) is clear from the definition of λ. To prove (f) observe that certainly $\lambda_{\mathfrak{p}}(\underset{\sim}{a}) \equiv 1 \pmod{\mathfrak{m}}$ if $a_{\mathfrak{p}} = 1$ since $\lambda_{\mathfrak{p}}(\underset{\sim}{a}) = \lambda(\underset{\sim}{a})$ in this case. Since $\lambda_{\mathfrak{p}}(\underset{\sim}{a}) = 1$ if $\underset{\sim}{a} = (\ldots,a,a,\ldots)$ with $a \in K^*$, (f) follows by continuity. To prove (g) it suffices, after Lemma 7 (iii), to prove that $\lambda \circ N_{F/K}$ satisfies (a) to (d) (with $M = F$) and that $\lambda_{\mathfrak{p}} \circ N_{F/K} = (\lambda \circ N_{F/K})_{\mathfrak{p}}$ takes values in $(1+\mathfrak{p}\mathfrak{O}_{K_{\mathfrak{p}}})^\times$. It is clear that (a) to (d) are indeed satisfied, as well as the values of $\lambda_{\mathfrak{p}} \circ N_{F/K}$ being congruent to 1 modulo $\mathfrak{m}$. Hence it suffices to show that $\lambda_{\mathfrak{p}} \circ N_{F/K}$ takes values in $K_{\mathfrak{p}}^*$, or equivalently that the restriction of $\lambda_{\mathfrak{p}}$ to the subgroup of J_K corresponding to F takes values in $K_{\mathfrak{p}}^*$. Now this subgroup is contained in the subgroup Z corresponding to the Hilbert class field H of K. If $a \in Z$ and $\underset{\sim}{a}_{\mathfrak{p}} = 1$, then $\iota(\underset{\sim}{a})$ is principal with generator prime to $\mathfrak{p}$, and so $\lambda_{\mathfrak{p}}(\underset{\sim}{a}) = \lambda(\underset{\sim}{a}) \in K_{\mathfrak{p}}^*$. Since $\lambda_{\mathfrak{p}}(\underset{\sim}{a}) = 1$ if $\underset{\sim}{a} = (\ldots,a,a,\ldots)$ with $a \in K^*$ the continuity of $\lambda_{\mathfrak{p}}$ implies that $\lambda_{\mathfrak{p}}(\underset{\sim}{a}) \in K_{\mathfrak{p}}$ for all $\underset{\sim}{a} \in Z$, which is (g). This completes the proof of Proposition 8.

Proof of Theorem B. — We first establish the identity

$$L^*((\psi\varepsilon^{-1})^k,\theta,s) = \prod_{\chi} L_\infty(s,k,\chi) \tag{25}$$

where the character used to define the $L_\infty(s,k,\chi)$'s is the character λ of Proposition 8 (ii) (or rather the homomorphism $\lambda: I(\mathfrak{p}) \to \bar{\mathbf{Q}}$ that it induces — which satisfies the properties (i) and (ii) (with $\mathfrak{f} = \mathfrak{p}$) given at the beginning of this section), and the product on the right is over all the characters of $\mathrm{Gal}(K^{ab}/K)$ whose restriction to $\mathrm{Gal}(K^{ab}/F)$ is θ. Let $\mathfrak{q} \neq \mathfrak{p}$ be a prime of K and $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_r$ the primes of F above $\mathfrak{q}$.

We observe that θ is either unramified at all the $\mathfrak{Q}'s$, or ramified at all of them and so we can speak of θ being ramified or unramified above $\mathfrak{q}$. Indeed, let M be the finite extension of F corresponding to the kernel of θ, so that M/K is abelian. Let I be the inertia field of $\mathfrak{q}$ in M. Then the Galois group $\mathrm{Gal}(M/I)$ (resp. $\mathrm{Gal}(M/FI)$ is the ramification group of $\mathfrak{q}$ (resp. of any $\mathfrak{Q}$ in F above $\mathfrak{q}$) in M/K. From this we see that θ is unramified above $\mathfrak{q}$ if and only if all the $\chi's$ are unramified at $\mathfrak{q}$: in fact it is clear that if θ is non-trivial on $\mathrm{Gal}(M/FI)$ then any χ is non-trivial on $\mathrm{Gal}(M/I)$. Conversely if θ is trivial on $\mathrm{Gal}(M/FI)$ then θ factors through $\mathrm{Gal}(FI/F)$ inducing a character θ_0 of $\mathrm{Gal}(I/I\cap F)$. Let us choose any prolongation of θ_0 to a character χ_0 of $\mathrm{Gal}(I/K)$: as a character of $\mathrm{Gal}(M/K)$ χ_0 is trivial on $\mathrm{Gal}(M/I)$ and its restriction to $\mathrm{Gal}(M/F)$ is our given θ.

Hence to establish (25) it suffices to compare Euler factors above primes $\mathfrak{q} \neq \mathfrak{p}$ of K where θ is unramified. Fix a $\chi_0 \in \mathrm{Gal}(M/K)$ whose restriction to $\mathrm{Gal}(M/F)$ is θ, and which is unramified at $\mathfrak{p}$. Write $X = \lambda^k(\mathfrak{q})\chi_0(\mathfrak{q})N\mathfrak{q}^{-s}$. Then if $\mathfrak{Q}$ is any prime of F above $\mathfrak{q}$, and f the residue class degree, then one finds that $X^f = (\psi\varepsilon^{-1})^k(\mathfrak{Q})\theta(\mathfrak{Q})N\mathfrak{Q}^{-s}$. Hence one is reduced to verifying the identity

$$(1-X^f)^g = \prod_{\tilde{\chi}} (1-\tilde{\chi}(\mathfrak{q})X)$$

where g is the number of primes of F above $\mathfrak{q}$ and $\tilde{\chi}$ runs over all the characters of $\mathrm{Gal}(F/K)$. But this is precisely the same identity needed to prove the analogue of (25) for Dirichlet L-series (see e.g. S. Lang, « Algebraic Number Theory », p. 230) and so (25) itself is proved. We define $L_{\mathfrak{p}}(\psi,\theta,s)$ to be the product

$$\prod_{\chi} L_{\mathfrak{p}}(s,\chi). \tag{26}$$

It is clear from (26) and Theorem 6 that $L_{\mathfrak{p}}(\psi,\theta,s)$ is locally meromorphic and satisfies the required formula at $s = k$, $k \geqslant 1$. Moreover it is locally analytic except perhaps when the trivial character appears in the product on the right hand side, and this happens if and only if θ is itself trivial, in which case there is at most a simple pole at $s = 0$. The existence of this pole will be proved in the next section.

4. A Formula for $L_p(0,\chi)$.

In this section we give a formula for the value of the function $L_p(s,\chi)$ introduced in § 3 at $s = 0$. In addition to the (complex) functions discussed in § 2, we define, for every lattice Λ, and $z \in \mathbf{C}$,

$$\Phi(z,\Lambda) = \exp(-6\eta(z,\Lambda)z)\,\Delta(\Lambda)\sigma^{12}(z,\Lambda). \tag{27}$$

This function is denoted by $\varphi^{(12)}(t,\Gamma)$ in Robert [23, p. 8] where $t = z$ and $\Gamma = \Lambda$. If $\lambda \in \mathbf{C}^*$ we have the homogeneity relation

$$\Phi(\lambda z,\lambda\Lambda) = \Phi(z,\Lambda); \tag{28}$$

moreover (10), (11) and the homogeneity property of $a(\Lambda)$ easily imply that if Λ' is a lattice containing Λ,

$$\theta(z,\Lambda;\Lambda') = \frac{\Phi(z,\Lambda)^{(\Lambda':\Lambda)}}{\Phi(z,\Lambda')}. \tag{29}$$

We shall need the following relations which are proved in [26, p. 9]. If n_1 is the exponent of the group Λ'/Λ, then

$$\prod_{\substack{z \in \Lambda' \bmod \Lambda \\ z \notin \Lambda}} \Phi(z,\Lambda)^{n_1} = \left[\frac{\Delta(\Lambda')}{\Delta(\Lambda)}\right]^{n_1}. \tag{30}$$

Furthermore, if $t \in f^{-1}\Lambda$, but $t \notin \Lambda$, and $m = (n_1, f)$, then

$$\prod_{z \in \Lambda' \bmod \Lambda} \Phi(t+z,\Lambda)^m = \Phi(t,\Lambda')^m. \tag{31}$$

The purpose of introducing the function Φ is that its values at points of $\mathbf{Q}\Lambda$ are algebraic numbers belonging to certain well-described fields (at least in the case when Λ has complex multiplication). If $\mathfrak{f}$ is an integral ideal of K we denote by $\iota(\mathfrak{f})$ the smallest positive integer contained in $\mathfrak{f}$; as in § 3, $I(\mathfrak{f})$ is the group of ideals prime to $\mathfrak{f}$, $P_{\mathfrak{f}}$ the subgroup consisting of those ideals having a generator $a \equiv 1 \pmod{\mathfrak{f}}$, $\Gamma(\mathfrak{f})$ denotes the quotient group $I(\mathfrak{f})/P_{\mathfrak{f}}$ while if $\mathfrak{a} \in I(\mathfrak{f})$ we write $\mathrm{Cl}_{\mathfrak{f}}(\mathfrak{a})$ for the image of $\mathfrak{a}$ in $\Gamma(\mathfrak{f})$. Let $A(\mathfrak{f})$ be the set of pairs $(a, \mathfrak{b})$ where $a \in K^*$ and $\mathfrak{b} \in I((1))$ such that $\mathfrak{f} = \{x \in \mathfrak{O}_K \mid ax \in \mathfrak{b}\}$. It is clear that if $(a,\mathfrak{b}) \in A(\mathfrak{f})$ then the ideal $(a)\mathfrak{f}\mathfrak{b}^{-1}$ is prime to $\mathfrak{f}$, and we write $\mathrm{Cl}_{\mathfrak{f}}(a,\mathfrak{b})$ for $\mathrm{Cl}_{\mathfrak{f}}((a)\mathfrak{f}\mathfrak{b}^{-1})$.

Consersely if $C \in \Gamma(\mathfrak{f})$ we can find $(a,\mathfrak{b}) \in A(\mathfrak{f})$ with $C = Cl_{\mathfrak{f}}(a,\mathfrak{b})$, while $Cl_{\mathfrak{f}}(a,\mathfrak{b}) = Cl_{\mathfrak{f}}(a',\mathfrak{b}')$ if and only if there exists $x \in K^*$ with $\mathfrak{b}' = x\mathfrak{b}$ and $a' - xa \in \mathfrak{b}'$. If $\mathfrak{f} \neq (1)$ and $C \in \Gamma(\mathfrak{f})$ we define a complex number $\Phi_{\mathfrak{f}}(C)$ by

$$\Phi_{\mathfrak{f}}(C) = \Phi(a,\mathfrak{b})^{\iota(\mathfrak{f})} \tag{32}$$

where $Cl_{\mathfrak{f}}(a,\mathfrak{b}) = C$.

The quantities (32) are known to enjoy the following properties (cf. [23]):

(i) They are algebraic integers belonging to the ray class field $H_{\mathfrak{f}}$ modulo $\mathfrak{f}$ of K, which are units if $\mathfrak{f}$ is divisible by at least two distinct primes of K, while if $\mathfrak{f} = \mathfrak{q}^r$, $\mathfrak{q}$ a prime then the ideal generated by $\Phi_{\mathfrak{f}}(C)$ is independent of C and only divisible by primes above $\mathfrak{q}$.

In view of (29), this justifies the remarks made in § 2, just before (14) and (15).

(ii) Writing $\sigma(C)$ for the element of $\mathrm{Gal}(H_{\mathfrak{f}}/K)$ corresponding to C, we have the explicit reciprocity law

$$\Phi_{\mathfrak{f}}(CC') = \Phi_{\mathfrak{f}}(C')^{\sigma(C)}. \tag{33}$$

We also need an analogue of (i) and (ii) when $\mathfrak{f} = (1)$. If $C \in \Gamma((1))$ and $Cl_{(1)}(\mathfrak{b}^{-1}) = C$, we define

$$\delta(C) = \left[\frac{\Delta(\mathfrak{b})}{\Delta(\mathfrak{O}_K)}\right]^{h_K} \beta^{12}, \tag{34}$$

where h_K is the class number of K and β is any generator of $\mathfrak{b}^{h_K}$. Then $\delta(C)$ belongs to the Hilbert class field $H_{(1)}$ of K and again we have the reciprocity law

$$\delta(CC') = \delta(C')^{\sigma(C)}\,\delta(C) \tag{35}$$

for all C, $C' \in \Gamma((1))$, where again $\sigma(C)$ is the element of $\mathrm{Gal}(H_{(1)}/K)$ corresponding to C (see [23, p. 24]; note however that his $\delta(C)$ is different from ours).

Finally we record a norm relation between the $\Phi_{\mathfrak{f}}(C)$'s and $\delta(C)$'s which is part of [23, Théorème 2], (and in any case follows easily from (30) and (31)). Let $m_K(\mathfrak{f})$ denote the number of roots of unity in K which are

congruent to 1 (mod $\mathfrak{f}$). Then if $\mathfrak{p} \nmid \mathfrak{f}$, one has since $\iota(\mathfrak{p}) \geqslant 5$

$$(36A)\quad m_K(\mathfrak{f}) \sum_{\substack{C' \in \Gamma(\mathfrak{fp}) \\ C' \to C \in \Gamma(\mathfrak{f})}} \log_p \Phi_{\mathfrak{fp}}(C') = \frac{\iota(\mathfrak{fp})}{\iota(\mathfrak{f})} \log_p \left(\frac{\Phi_{\mathfrak{f}}(C)}{\Phi_{\mathfrak{f}}(C\mathrm{Cl}_{\mathfrak{f}}(\mathfrak{p}^{-1}))} \right) \quad \text{if } \mathfrak{f} \neq (1),$$

$$(36B)\quad = \iota(\mathfrak{p})(h_K)^{-1} \log_p \left(\frac{\delta(C)}{\delta(C\mathrm{Cl}_{(1)}(\mathfrak{p}^{-1}))} \right)$$

if $\mathfrak{f} = (1)$, where the sum on the left is taken over all the $C' \in \Gamma(\mathfrak{fp})$ whose image in $\Gamma(\mathfrak{f})$ is C.

Now let χ be a character of finite order on $\mathrm{Gal}(K^{ab}/K)$ and $\mathfrak{f}$ its conductor. If $\gamma \in K$ has denominator exactly $\mathfrak{f}$ we define the Gauss sum $G(\chi)$ by

$$(37)\quad G(\chi) = \chi((\gamma)\mathfrak{f}) \sum_{x \in (\mathfrak{O}_K/\mathfrak{f})^*} \chi((x)) \exp\left(2\pi i \mathrm{Tr}\left(\frac{\gamma x}{\sqrt{d_K}} \right) \right) \quad \text{if } \mathfrak{f} \neq (1)$$
$$= 1 \quad \text{if } \mathfrak{f} = (1),$$

where the sum is taken over a set of representatives $\{x\}$ in $\mathfrak{O}_K$ of $(\mathfrak{O}_K/\mathfrak{f})^*$, and Tr is the trace from K to $\mathbf{Q}$. Since $\mathrm{Tr}\left(\frac{y}{\sqrt{d_K}} \right) \in \mathbf{Z}$ for all $y \in \mathfrak{O}_K$, we see that $G(\chi)$ does not depend on the choice of representatives $\{x\}$. Also $G(\chi)$ does not depend on the choice of γ, for if γ' also has exact denominator $\mathfrak{f}$ we can find $\alpha \in \mathfrak{O}_K$ with $((\alpha),\mathfrak{f}) = (1)$ and $\gamma - \alpha\gamma' \in \mathfrak{O}_K$. Therefore $\chi((\gamma)\mathfrak{f}) = \chi((\alpha\gamma')\mathfrak{f})$ and $\mathrm{Tr}\left(\frac{\gamma x}{\sqrt{d_K}} \right) \equiv \mathrm{Tr}\left(\frac{\alpha\gamma' x}{\sqrt{d_K}} \right) (\mathrm{mod}\ \mathbf{Z})$ and so

$$G(\chi) = \chi((\alpha\gamma')\mathfrak{f}) \sum_{x \in (\mathfrak{O}_K/\mathfrak{f})^*} \chi(x)) \exp\left(2\pi i \,\mathrm{Tr}\left(\frac{\alpha\gamma' x}{\sqrt{d_K}} \right) \right)$$
$$= \chi((\gamma')\mathfrak{f}) \sum_{x \in (\mathfrak{O}_K/\mathfrak{f})^*} \chi((\alpha x)) \exp\left(2\pi i \,\mathrm{Tr}\left(\frac{\alpha\gamma' x}{\sqrt{d_K}} \right) \right)$$

and so the assertion follows on replacing αx by x.

We need one final definition before stating the main result of this section. We write

$$(38)\quad S(\chi) = \frac{1}{h_K} \sum_{C \in \Gamma((1))} \chi^{-1}(C) \log_p \delta(C) \quad \text{if } \mathfrak{f} = (1)$$
$$= \sum_{C \in \Gamma(\mathfrak{f})} \chi^{-1}(C) \log_p \Phi_{\mathfrak{f}}(C) \quad \text{if } \mathfrak{f} \neq (1).$$

THEOREM 9. — *Let* χ *be a non-trivial character of finite order on* $\mathrm{Gal}(K^{ab}/K)$ *and* $\mathfrak{f}$ *be its conductor. Let* $m_K(\mathfrak{f})$ *be the number of roots of unity in* K *which are congruent to* $1 \pmod{\mathfrak{f}}$, $\iota(\mathfrak{f})$ *be the least positive integer which belongs to* $\mathfrak{f}$, *and* $G(\chi)$ *be defined by* (37) *and* (38) *respectively. Then we have*

$$L_{\mathfrak{p}}(0,\chi) = -\frac{1}{12}\frac{1}{\iota(\mathfrak{f})N\mathfrak{f}m_K(\mathfrak{f})}\left(1-\frac{\chi(\mathfrak{p})}{N\mathfrak{p}}\right)G(\chi)S(\chi),$$

where we interpret $\chi(\mathfrak{p})$ *as* 0 *if* $\mathfrak{p}|\mathfrak{f}$.

Proof. — Let $\mathfrak{f}^*$ be the least common multiple of $\mathfrak{f}$ and the conductor of λ. According to Proposition 8 (ii), $\mathfrak{f}^* = \mathfrak{f}$ or $\mathfrak{f}\mathfrak{p}$ according as to whether $\mathfrak{p}$ divides $\mathfrak{f}$ or not. Let N be the order of $\Gamma(\mathfrak{f}^*)$ and $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_N$ a set of mutually coprime integral ideals in $I(\mathfrak{f}^*)$ representing the elements of $\Gamma(\mathfrak{f}^*)$. For each i, let a_i be a fixed solution of the congruences $a \equiv 0 \pmod{\mathfrak{a}_i}$ and $a \equiv 1 \pmod{\mathfrak{f}^*}$. We say that $x_i \in K$ is primitive if it has exact denominator $\mathfrak{a}_i\mathfrak{f}^*$, i.e.

$$(x_i) = \mathfrak{b}_i(\mathfrak{a}_i\mathfrak{f}^*)^{-1} \qquad \text{with} \qquad (\mathfrak{b}_i, \mathfrak{a}_i\mathfrak{f}^*) = (1).$$

We need

LEMMA 10. — *We can choose primitive* $x_i's$ *in such a way that*

(i) $x_i a_i - x_j a_j \in \mathfrak{O}_K$ *for all* $i, j = 1, 2, \ldots, N$, *and*

(ii) *There exists* $C_0 \in \Gamma(\mathfrak{f}^*)$ *independent of* i *such that*

$$\mathrm{Cl}_{\mathfrak{f}^*}(\mathfrak{b}_i) = \mathrm{Cl}_{\mathfrak{f}^*}(\mathfrak{a}_i)C_0$$

for all i.

Proof. — Since the $\mathfrak{a}_i's$ are coprime, we can find for each i an integral ideal $\mathfrak{b}_i$ prime to $\mathfrak{f}^*$ and to all the $\mathfrak{a}_i's$ such that $\left(\prod_{j\neq i}\mathfrak{a}_j\right)\mathfrak{b}_i \in P_{\mathfrak{a}_i\mathfrak{f}^*}$. Since $\mathfrak{p}|\mathfrak{f}^*$ and $\iota(\mathfrak{p}) \geqslant 5$, $\left(\prod_{j\neq i}\mathfrak{a}_j\right)\mathfrak{b}_i$ has a unique generator α_i such that $\alpha_i \equiv 1 \pmod{\mathfrak{f}^*}$ and $\alpha_i \equiv 1 \pmod{\mathfrak{a}_i}$. Then if $i \neq j$

$$\alpha_i - \alpha_j \in \left(\prod_{k\neq i,j}\mathfrak{a}_k\right)\mathfrak{f}^*$$

but $\alpha_i \not\equiv \alpha_j \pmod{\mathfrak{a}_i\mathfrak{a}_j}$. Let $\mathfrak{b}$ be an integral ideal prime to all the $\mathfrak{a}_i's$ and

to $\mathfrak{f}^*$ such that $\left(\prod_{i=1}^{N} \mathfrak{a}_i\right)\mathfrak{f}^* \mathfrak{b}^{-1}$ is principal with generator β, and define

$$x_i = \frac{\alpha_i}{\beta} \qquad \text{for each} \qquad i = 1, 2, \ldots, N.$$

Then $(x_i) = \mathfrak{b}_i \mathfrak{b}(\mathfrak{a}_i \mathfrak{f}^*)^{-1}$, say, with $(\mathfrak{b}_i \mathfrak{b}, \mathfrak{a}_i \mathfrak{f}^*) = (1)$ so that the $x_i's$ are primitive and $\mathfrak{h}_i = \mathfrak{b}_i \mathfrak{b}$. Also

$$x_i - x_j = \frac{\alpha_i - \alpha_j}{\beta} \in \mathfrak{b}(\mathfrak{a}_i \mathfrak{a}_j)^{-1} \subseteq (\mathfrak{a}_i \mathfrak{a}_j)^{-1}$$

and since $a_i \in \mathfrak{a}_i$ and $a_i = 1 + \beta_i$ for some $\beta_i \in \mathfrak{f}^*$ we see that in the decomposition

$$x_i a_i - x_j a_j = (x_i - x_j) + (x_i \beta_i - x_j \beta_j)$$

the right hand side lies in $(\mathfrak{a}_i \mathfrak{a}_j)^{-1}$ while the left hand side belongs to $\mathfrak{f}^{*-1}$. Therefore $x_i a_i - x_j a_j \in \mathfrak{O}_K$ because the $\mathfrak{a}_i's$ and $\mathfrak{f}^*$ are coprime.

Finally since $\alpha_i \equiv 1 \pmod{\mathfrak{f}^*}$, $\mathrm{Cl}_{\mathfrak{f}^*}(\mathfrak{b}_i) = \mathrm{Cl}_{\mathfrak{f}^*}(\mathfrak{a}_i)\left(\mathrm{Cl}_{\mathfrak{f}^*}\left(\prod_{i=1}^{N} \mathfrak{a}_i\right)\right)^{-1}$, so that

$$\mathrm{Cl}_{\mathfrak{f}^*}(\mathfrak{h}_i) = \mathrm{Cl}_{\mathfrak{f}^*}(\mathfrak{a}_i) C_0$$

with $C_0 = \mathrm{Cl}_{\mathfrak{f}^*}(\mathfrak{b})\left(\mathrm{Cl}_{\mathfrak{f}^*}\left(\prod_{i=1}^{N} \mathfrak{a}_i\right)\right)^{-1}$. This completes the proof of Lemma 10.

We now evaluate $L_p(0,\chi)$. Let S be as in § 2 (with $\mathfrak{b} = \mathfrak{f}^*$), i.e. S is a set of pairs $(\mathfrak{c}, a_\mathfrak{c})$ with $\mathfrak{c} \in \Sigma$ and $a_\mathfrak{c}$ satisfying $\sum_{\mathfrak{c}} (N\mathfrak{c} - 1) a_\mathfrak{c} = 0$. We now further suppose that the $\mathfrak{c}'s$ are prime to $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_N$ and moreover that $\sum_{\mathfrak{c}} (1 - \chi(\mathfrak{c})) a_\mathfrak{c} \neq 0$. To satisfy this last condition, we need only take an S consisting of two pairs $(\mathfrak{c}, a_\mathfrak{c})$ and $(\mathfrak{c}', a_{\mathfrak{c}'})$ with $a_\mathfrak{c} = N\mathfrak{c}' - 1$ and $a_{\mathfrak{c}'} = -(N\mathfrak{c} - 1)$; choose $\mathfrak{c}$ so that $\chi(\mathfrak{c}) \neq 1$ and then $\mathfrak{c}'$ so that $N\mathfrak{c}' - 1 > \dfrac{2(N\mathfrak{c} - 1)}{|1 - \chi(\mathfrak{c})|}$. Let $\delta_\mathfrak{c}$ be an integer such that $N\mathfrak{c}\,\delta_\mathfrak{c} \equiv 1 \pmod{\mathfrak{f}^*}$, so that $N\mathfrak{c}\,\delta_\mathfrak{c} a_i \equiv 1 \pmod{\mathfrak{f}^*}$ and $N\mathfrak{c}\,\delta_\mathfrak{c} a_i \in \mathfrak{a}_i \mathfrak{c}$. Consider for $s \in \mathbf{Z}_p$, $s \neq 0$, the expression

$$(39) \qquad \sum_{i=1}^{N} \frac{N\mathfrak{a}_i}{(\lambda(\mathfrak{a}_i))^s \chi(\mathfrak{a}_i)} \sum_{\mathfrak{c}} (G_p(a_i, s, \mathfrak{a}_i \mathfrak{f}^*) - G_p(N\mathfrak{c}\,\delta_\mathfrak{c} a_i, s, \mathfrak{a}_i \mathfrak{f}^* \mathfrak{c})) N\mathfrak{c} a_\mathfrak{c}$$

which is equal to

$$(40)\quad \sum_{\mathfrak{c}}\Bigg[N\mathfrak{c}\sum_{i=1}^{N}\frac{N\mathfrak{a}_i}{(\lambda(\mathfrak{a}_i))^s\chi(\mathfrak{a}_i)}G_p(a_i,s,\mathfrak{a}_i\mathfrak{f}^*) - (\lambda(\mathfrak{c}))^s\chi(\mathfrak{c})\sum_{i=1}^{N}\frac{N\mathfrak{a}_i\mathfrak{c}}{(\lambda(\mathfrak{a}_i\mathfrak{c}))^s\chi(\mathfrak{a}_i\mathfrak{c})}G_p(N\mathfrak{c}\,\delta_{\mathfrak{c}}a_i,s,\mathfrak{a}_i\mathfrak{f}^*\mathfrak{c})\Bigg]a_{\mathfrak{c}}$$

which simplifies, in view of the calculations leading up to (22) of the previous section, to

$$\Bigg[\sum_{\mathfrak{c}}(N\mathfrak{c}-(\lambda(\mathfrak{c}))^s\chi(\mathfrak{c}))a_{\mathfrak{c}}\Bigg]L_p(s,\chi)$$

which, by virtue of the relation $\sum_{\mathfrak{c}}(N\mathfrak{c}-1)a_{\mathfrak{c}}=0$, can be written as

$$(41)\qquad \Bigg[\sum_{\mathfrak{c}}(1-(\lambda(\mathfrak{c}))^s\chi(\mathfrak{c}))a_{\mathfrak{c}}\Bigg]L_p(s,\chi).$$

On the other hand we have for $s\neq 0$

$$-12N\mathfrak{a}_i\mathfrak{f}^*\sum_{\mathfrak{c}}(G_p(a_i,s,\mathfrak{a}_i\mathfrak{f}^*)-G_p(N\mathfrak{c}\,\delta_{\mathfrak{c}}a_i,s,\mathfrak{a}_i\mathfrak{f}^*\mathfrak{c})N\mathfrak{c})a_{\mathfrak{c}}=G_p(a_i,s,\mathfrak{a}_i\mathfrak{f}^*,S).$$

This is true for $s=k\in\mathbf{Z}$, $k\geqslant 1$ by (20) and the definition of $G_p(a,s,\mathfrak{g},S)$ and $G_p(a,s,\mathfrak{g})$ and follows for arbitrary $s\neq 0$ by continuity, and so the equality of (39) and (41) implies that

$$-\frac{1}{12N\mathfrak{f}^*}\sum_{i=1}^{N}\frac{G_p(a_i,s,\mathfrak{a}_i\mathfrak{f}^*,S)}{\lambda(\mathfrak{a}_i)^s\chi(\mathfrak{a}_i)}=\Bigg[\sum_{\mathfrak{c}}(1-\lambda(\mathfrak{c})^s\chi(\mathfrak{c}))a_{\mathfrak{c}}\Bigg]L_p(s,\chi).$$

This equality is valid also for $s=0$ since both sides remain bounded as $s\to 0$. Hence taking $s=0$ and using (19) we obtain

$$(42)\quad [\Sigma(1-\chi(\mathfrak{c}))a_{\mathfrak{c}}]L_p(0,\chi)=-\frac{1}{12N\mathfrak{f}^*}\sum_{i=1}^{N}\chi(\mathfrak{a}_i)^{-1}f_i(0,S),$$

where $f_i(T,S)$ is the function $f_{\hat{\rho}}(T,S)$ of § 2 with $\mathfrak{g}$ replaced by $\mathfrak{a}_i\mathfrak{f}^*$ and $\hat{\rho}$ by $\bar{a}_i\Omega$. Thus the proof of Theorem 9 involves the evaluation of $f_i(0,S)$ and rearranging the right hand side of (42).

Now in $\mathbf{C}_p[[T]]$ we have

$$f_i(T,S)=\sum_{\substack{\rho\in a_i^{-1}\mathfrak{f}^{*-1}\mathscr{L}\\ \bmod\mathscr{L}}}f_i(T,\rho,S)\langle\rho,\bar{a}_i\Omega\rangle_{\mathscr{L}}$$

where $f_i(T,\rho,S)$ is the function $f(T,\rho,S)$ of (15) with $g = a_i\mathfrak{f}^*$. Also if $\rho = x\Omega \notin \mathscr{L}$ then

$$f(0,\rho,S) = \log_p \prod_{\mathfrak{c}} \left(\frac{\Phi(x,\mathfrak{O}_K)^{N\mathfrak{c}}}{\Phi(x,\mathfrak{c}^{-1})} \right)^{a_\mathfrak{c}} = \sum_{\mathfrak{c}} (\log_p \Phi(x,\mathfrak{O}_K)N\mathfrak{c} - \log_p \Phi(x,\mathfrak{c}^{-1}))a_\mathfrak{c};$$

on the other hand $f_i(0,0,S) = \log_p \left(\prod_{\mathfrak{c}} \frac{\Delta(\mathscr{L})^{N\mathfrak{c}}}{\Delta(\mathfrak{c}^{-1}\mathscr{L})} \right)^{a_\mathfrak{c}}$ is independent of i, and so $\sum_{i=1}^{N} \chi(a_i^{-1}) f_i(0,0,S) = 0$. Taking all this into account we find that $\sum_{\mathfrak{c}} (1-\chi(\mathfrak{c}))a_\mathfrak{c} L_p(0,\chi)$ is equal to

$$(43) \quad -\frac{1}{12N\mathfrak{f}^*} \sum_{i=1}^{N} \chi(a_i)^{-1} \sum_{x}{}' \langle x,\bar{a}_i \rangle_{\mathfrak{O}_K} \sum_{\mathfrak{c}} (\log_p \Phi(x,\mathfrak{O}_K)N\mathfrak{c} - \log_p \Phi(x,\mathfrak{c}^{-1}))a_\mathfrak{c}$$

where x runs over a set of representatives of the non-zero elements of $(a_i\mathfrak{f}^*)^{-1}/\mathfrak{O}_K$, and so the rest of the proof consists of simplifying (43). To this end we consider the sum

$$\sum_{i=1}^{N} \chi(a_i^{-1}) \sum_{x}{}' \langle x,\bar{a}_i \rangle_{\mathfrak{O}_K} \log_p \Phi(x,\mathfrak{c}^{-1})$$

where $\mathfrak{c}$ is now either one of the ideals appearing in S or $\mathfrak{c} = (1)$. From now on we write $\langle z,w \rangle$ for $\langle z,w \rangle_{\mathfrak{O}_K}$. We fix $x_1, x_2, \ldots, x_N$ as in Lemma 10 and observe that $\langle x_i,\bar{a}_i \rangle = \langle x_i a_i,1 \rangle$ and so the expression becomes

$$(44) \quad \sum_{i=1}^{N} \chi(a_i^{-1}) \sum_{\substack{z \in \mathfrak{O}_K/a_i\mathfrak{f}^* \\ z \neq 0}}{}' \langle x_i a_i z,1 \rangle \log_p \Phi(x_i z,\mathfrak{c}^{-1}).$$

Since $x_i a_i - x_j a_j \in \mathfrak{O}_K$ by Lemma 10, the term $\langle x_i a_i z,1 \rangle$ is independent of i and we can choose $\lambda \in \mathfrak{f}^{*-1}$ such that $\langle \lambda,1 \rangle = \langle x_i a_i,1 \rangle$ for all i. Moreover if $y \in (\mathfrak{O}_K/\mathfrak{f}^*)$ we have, by (30) and (31)

$$\sum_{z \mapsto y} \log_p \Phi(x_i z,\mathfrak{c}^{-1}) = \log_p \Phi(x_i y, a_i^{-1}\mathfrak{c}^{-1}) \quad \text{if} \quad y \neq 0$$

$$= \log_p \left(\frac{\Delta(a_i^{-1}\mathfrak{c}^{-1})}{\Delta(\mathfrak{c}^{-1})} \right) \quad \text{if} \quad y = 0$$

where the sum is taken over all $z \in (\mathfrak{O}_K/a_i\mathfrak{f}^*)$ with $z \neq 0$ whose image in

$(\mathfrak{O}_K/\mathfrak{f}^*)$ is y. For each ideal $\mathfrak{g}$ dividing $\mathfrak{f}^*$, let

$$\tilde{Y}_\mathfrak{g} = \left\{ y \in \mathfrak{O}_K \mid y \neq 0 \quad \text{and} \quad (y) = \frac{\mathfrak{f}^*}{\mathfrak{g}} \mathfrak{h}_y \quad \text{with} \quad (\mathfrak{h}_y, \mathfrak{f}^*) = (1) \right\}.$$

It is clear that $\mathfrak{O}_K \setminus \{0\} = \bigcup_{\mathfrak{g} \mid \mathfrak{f}^*} \tilde{Y}_\mathfrak{g}$ (disjoint union) and if $y, y' \in \mathfrak{O}_K \setminus \{0\}$ with $y \equiv y' \pmod{\mathfrak{f}^*}$ then y and y' belong to the same $\tilde{Y}_\mathfrak{g}$. Therefore the image $Y_\mathfrak{g}$ of $\tilde{Y}_\mathfrak{g}$ in $(\mathfrak{O}_K/\mathfrak{f}^*)$ is well-defined. Thus (44) splits up as the sum over $\mathfrak{g} \mid \mathfrak{f}^*$ of the expressions

$$\text{(45A)} \quad \sum_{i=1}^{N} \chi(\mathfrak{a}_i^{-1}) \sum_{y \in Y_\mathfrak{g}} \langle \lambda y, 1 \rangle \log_p \Phi(x_i y, \mathfrak{a}_i^{-1} \mathfrak{c}^{-1}) \quad \text{if} \quad \mathfrak{g} \neq (1)$$

and

$$\text{(45B)} \quad \sum_{i=1}^{N} \chi(\mathfrak{a}_i^{-1}) \log_p \frac{\Delta(\mathfrak{a}_i^{-1} \mathfrak{c}^{-1})}{\Delta(\mathfrak{c}^{-1})} \quad \text{if} \quad \mathfrak{g} = (1).$$

If $(x_i) = \mathfrak{h}_i \mathfrak{a}_i^{-1} \mathfrak{f}^{*-1}$ and $(y) = \mathfrak{f}^* \mathfrak{g}^{-1} \mathfrak{h}_y$, then, recalling the definitions given just before (32), we have

$$\mathrm{Cl}_\mathfrak{g}(x_i y, \mathfrak{a}_i^{-1} \mathfrak{c}^{-1}) = \mathrm{Cl}_\mathfrak{g}(\mathfrak{h}_i \mathfrak{h}_y \mathfrak{c}) = \mathrm{Cl}_\mathfrak{g}(\mathfrak{a}_i \mathfrak{h}_y \mathfrak{c}) C_{0,\mathfrak{g}},$$

(using Lemma 10) where $C_{0,\mathfrak{g}}$ is the image of C_0 in $\Gamma(\mathfrak{g})$. Hence (45A) can be rewritten as

$$\frac{1}{\iota(\mathfrak{g})} \sum_{i=1}^{N} \chi(\mathfrak{a}_i^{-1}) \left\{ \sum_{y \in Y_\mathfrak{g}} \langle \lambda y, 1 \rangle \log_p \Phi_\mathfrak{g}(\mathrm{Cl}_\mathfrak{g}(\mathfrak{a}_i \mathfrak{h}_y \mathfrak{c}) C_{0,\mathfrak{g}}) \right\}$$

or, writing $C = \mathrm{Cl}_\mathfrak{g}(\mathfrak{a}_i \mathfrak{h}_y \mathfrak{c}) C_{0,\mathfrak{g}}$ and replacing the sum over the $\mathfrak{a}_i$ by that over $C \in \Gamma(\mathfrak{f}^*)$

$$\text{(46)} \quad \frac{1}{\iota(\mathfrak{g})} \chi(\mathfrak{c} C_0) \left(\sum_{y \in Y_\mathfrak{g}} \langle \lambda y, 1 \rangle \chi(\mathfrak{h}_y) \right) \left(\sum_{C \in \Gamma(\mathfrak{f}^*)} \chi(C^{-1}) \log_p \Phi_\mathfrak{g}(C) \right)$$

where we have written $\Phi_\mathfrak{g}(C)$ for $\Phi_\mathfrak{g}(C')$ for any class $C \in \Gamma(\mathfrak{f}^*)$ whose image in $\Gamma(\mathfrak{g})$ is C'.

If we take $|S|$ copies of (46) with $\mathfrak{c} = 1$ and subtract the sum of $a_\mathfrak{c} \times$ (46) as $(\mathfrak{c}, a_\mathfrak{c})$ runs over S, and divide by $\sum_\mathfrak{c} (1 - \chi(\mathfrak{c})) a_\mathfrak{c}$ (which is non-zero by our choice of S), we obtain

$$\text{(47A)} \quad \frac{1}{\iota(\mathfrak{g})} \chi(C_0) \left(\sum_{y \in Y_\mathfrak{g}} \langle \lambda y, 1 \rangle \chi(\mathfrak{h}_y) \right) \left(\sum_{C \in \Gamma(\mathfrak{f}^*)} \chi(C^{-1}) \log_p \Phi_\mathfrak{g}(C) \right)$$

(where $\mathfrak{g} \neq (1)$). Applying similar reasoning with (45B) (case $\mathfrak{g} = (1)$) gives (after dividing by $\sum_{\mathfrak{c}} (1 - \chi(\mathfrak{c})a_{\mathfrak{c}})$)

$$\text{(47B)} \qquad \frac{1}{h_K} \sum_{C \in \Gamma(\mathfrak{f}^*)} \chi(C^{-1}) \log_p \delta(C), \qquad (\mathfrak{g} = (1))$$

where again we have written $\delta(C)$ instead of $\delta(C')$ for any class $C \in \Gamma(\mathfrak{f}^*)$ whose image in $\Gamma((1))$ is C'. Hence $r_{,p}(0,\chi)$ is equal to $-\frac{1}{12N\mathfrak{f}^*}$ (the sum of the (47A)'s and (47B)'s, as $\mathfrak{g}$ runs over all the divisors of $\mathfrak{f}^*$).

We now show that (47A) and (47B) vanish except perhaps when $\mathfrak{g} = \mathfrak{f}$ or $\mathfrak{g} = \mathfrak{f}^*$. Since $\mathfrak{f}$ is the exact conductor of χ, this is the same as saying that χ does not factor through to a character of $\Gamma(\mathfrak{g})$, i.e. the restriction of χ to the kernel of the natural mapping $\Gamma(\mathfrak{f}^*) \to \Gamma(\mathfrak{g})$ is non-trivial, and so for each $C' \in \Gamma(\mathfrak{g})$, the sum $\Sigma\chi(C)$ taker over all C in $\Gamma(\mathfrak{f}^*)$ whose image in $\Gamma(\mathfrak{g})$ is C' vanishes. Since $\log_p \Phi_{\mathfrak{g}}(C)$ and $\log_p \delta(C)$ depend only on C', we deduce that (47A) and (47B) vanish for these $\mathfrak{g}$.

To complete the proof of Theorem 9 we need to evaluate (47A) and (47B) when $\mathfrak{g} = \mathfrak{f}$ or $\mathfrak{g} = \mathfrak{f}^*$, and consider separately the three cases (*a*) $\mathfrak{g} = \mathfrak{f} = (1)$, (*b*) $\mathfrak{g} = \mathfrak{f} \neq (1)$ and (*c*) $\mathfrak{p} \nmid \mathfrak{f}$ and $\mathfrak{g} = \mathfrak{f}^* = \mathfrak{p}\mathfrak{f}$.

(*a*) In this case $\mathfrak{f}^* = \mathfrak{p}$ and we have

$$\sum_{C \in \Gamma(\mathfrak{f}^*)} \chi(C^{-1}) \log_p \delta(C) = \frac{|\Gamma(\mathfrak{f}^*)|}{|\Gamma(1)|} \sum_{C' \in \Gamma((1))} \chi(C'^{-1}) \log_p \delta(C')$$

and since $|\Gamma((1))| = h_K$, $|\Gamma(\mathfrak{f}^*)| = |\Gamma(\mathfrak{p})| = \frac{h_K(N\mathfrak{p}-1)}{m_K}$ we find that (47B) reduces to (recalling the definition of $G(\chi)$ and $S(\chi)$ when $\mathfrak{f} = (1)$)

$$\text{(48)} \qquad \frac{N\mathfrak{p} - 1}{m_K} G(\chi)S(\chi).$$

In order to discuss (*b*) and (*c*) we need

LEMMA 11. — *We have*

$$G(\chi) = \chi(C_0) \sum_{y \in Y_{\mathfrak{f}}} \langle \lambda y, 1 \rangle \chi(\mathfrak{b}_y),$$

where λ *is as defined just after* (44).

Proof. — Fix $y_0 \in Y_\mathfrak{f}$ so that $Y_\mathfrak{f}$ can be identified with $\{y_0\xi \mid \xi \in (\mathfrak{O}_K/\mathfrak{f})^*\}$, and

$$\chi(C_0) \sum_{y \in Y_\mathfrak{f}} \langle \lambda y, 1\rangle \chi(\mathfrak{h}_y) = \chi(C_0\mathfrak{h}_{y_0}) \sum_{\xi \in (\mathfrak{O}_K/\mathfrak{f})^*} \langle \lambda y_0\xi, 1\rangle \chi((\xi)).$$

We may choose λ specifically to be x_1a_1, and if $\gamma = \lambda y_0$ then γ has exact denominator $\mathfrak{f}$; then

$$\langle \lambda y_0\xi, 1\rangle = \exp\left(2\pi i\left(\frac{\gamma\xi - \bar{\gamma}\bar{\xi}}{\sqrt{|d_K|}}\right)\right) = \exp\left(2\pi i \mathrm{Tr}\left(\frac{\gamma\xi}{\sqrt{d_K}}\right)\right).$$

On the other hand $(\gamma)\mathfrak{f} = (x_1a_1)\mathfrak{f}^*\mathfrak{f}^{-1}\mathfrak{h}_{y_0}\mathfrak{f} = \mathfrak{b}_1\mathfrak{b}(\mathfrak{a}_1^{-1})\mathfrak{h}_{y_0}(a_1)$ in the notation of the proof of Lemma 10, and so since $a_1 \equiv 1 \pmod{\mathfrak{f}}$,

$$\mathrm{Cl}_\mathfrak{f}((y)\mathfrak{f}) = \mathrm{Cl}_\mathfrak{f}(\mathfrak{b}_1\mathfrak{b}\mathfrak{a}_1^{-1}\mathfrak{h}_{y_0}).$$

But $C_{0,\mathfrak{f}} = \mathrm{Cl}_\mathfrak{f}\left(\mathfrak{b}\prod_{i=1}^{N}\mathfrak{a}_i^{-1}\right) = \mathrm{Cl}_\mathfrak{f}(\mathfrak{b}_1\mathfrak{b}\mathfrak{a}_1^{-1})$ since $\alpha_1 \equiv 1 \pmod{\mathfrak{f}}$ and the Lemma follows.

We now return to the proof of Theorem 9, and in particular discuss case (*b*). In fact, by an argument similar to that in (*a*) together with Lemma 11, (47A) becomes, on recalling the definition of $S(\chi)$

$$\frac{1}{m_K(\mathfrak{f})\iota(\mathfrak{f})}(N\mathfrak{p}-1)G(\chi)S(\chi) \tag{49}$$

if $\mathfrak{f}^* = \mathfrak{f}\mathfrak{p}$, and

$$\frac{1}{m_K(\mathfrak{f})\iota(\mathfrak{f})}G(\chi)S(\chi) \tag{50}$$

if $\mathfrak{f}^* = \mathfrak{f}$.

Finally we deal with case (*c*). We shall show that

$$\chi(C_0) \sum_{y \in Y_{\mathfrak{f}^*}} \langle \lambda y, 1\rangle \chi(\mathfrak{h}_y) = -\chi(\mathfrak{p})G(\chi) \tag{51}$$

and that

$$\sum_{C \in \Gamma(\mathfrak{f}^*)} \chi(C^{-1}) \log_p \Phi_{\mathfrak{f}^*}(C) = \frac{\iota(\mathfrak{f}^*)}{\iota(\mathfrak{f})m_K(\mathfrak{f})}(1-\chi^{-1}(\mathfrak{p})S(\chi)) \tag{52}$$

so that (47A) is equal to

$$\frac{1}{m_K(\mathfrak{f})\iota(\mathfrak{f})}(1-\chi(\mathfrak{p}))G(\chi)S(\chi). \tag{53}$$

To prove (51), let ξ be a fixed solution of the congruences $\xi \equiv 1 \pmod{\mathfrak{p}}$ and $\xi \equiv 0 \pmod{\mathfrak{f}}$. Then multiplication by $1-\xi$ gives rise to a natural mapping from $Y_{\mathfrak{f}\mathfrak{p}}$ onto $Y_{\mathfrak{f}}$, and

$$\sum_{y \mapsto z} \langle \lambda y, 1\rangle = -\langle \lambda z, 1\rangle$$

where the sum is taken over all y in $Y_{\mathfrak{f}\mathfrak{p}}$ whose image in $Y_{\mathfrak{f}}$ is z. On the other hand for these y, we have

$$\chi(\mathfrak{b}_y) = \chi(\mathfrak{p}\mathfrak{b}_z) = \chi(\mathfrak{p})\chi(\mathfrak{b}_z)$$

since $\mathfrak{f}$ is the conductor of χ. Taking the sum over all $z \in Y_{\mathfrak{f}}$ and using Lemma 11 we obtain (51). On the other hand the left hand side of (52) is equal to

$$\sum_{C' \in \Gamma(\mathfrak{f})} \chi(C'^{-1}) \sum_{\substack{C \in \Gamma(\mathfrak{f}\mathfrak{p}) \\ C \mapsto C'}} \log_p \Phi_{\mathfrak{f}\mathfrak{p}}(C).$$

Invoking (36) and writing $C_{\mathfrak{p}}$ for $Cl_{\mathfrak{f}}(\mathfrak{p})$, this becomes (if $\mathfrak{f} \neq (1)$)

$$\frac{\iota(\mathfrak{f}\mathfrak{p})}{\iota(\mathfrak{f})} \sum_{C' \in \Gamma(\mathfrak{f})} \chi(C'^{-1}) \log_p \left[\frac{\Phi_{\mathfrak{f}}(C')}{\Phi_{\mathfrak{f}}(C'C_{\mathfrak{p}}^{-1})}\right];$$

and using (33) we see that this equals the right hand side of (52). If $\mathfrak{f} = (1)$ we obtain the same result using (35) instead of (33).

In view of the fact that $L_{\mathfrak{p}}(0,\chi) = -\frac{1}{12N_{\mathfrak{f}}^{\mathfrak{p}}} \times$ (the sum of the (47A)'s and (47B)'s as $\mathfrak{g}$ varies over all the divisors of $\mathfrak{f}\mathfrak{p}$) Theorem 9 follows easily from these formulae. If $\mathfrak{f} = (1)$ then $\mathfrak{f}\mathfrak{p} = \mathfrak{p}$ and we use (48) and (53). If $\mathfrak{f} \neq (1)$ and $\mathfrak{p} \nmid \mathfrak{f}$ then $\mathfrak{f}\mathfrak{p} = \mathfrak{f}\mathfrak{p}$ and we use (49) and (53), while if $\mathfrak{p} \mid \mathfrak{f}$, so that $\mathfrak{f}\mathfrak{p} = \mathfrak{f}$ we use (50) together with $\chi(\mathfrak{p}) = 0$.

Completion of the Proof of Theorem B (sketch). – It suffices to show that $L_{\mathfrak{p}}(0,\chi) \neq 0$ if χ is non-trivial, and this is done in much the same way as the cyclotomic analogue (a full account of which may be found in [3]). Let $R_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic regulator of $H_{\mathfrak{f}}$ which, according to a theorem

of Brumer [3] is non-zero. One can show that $R_p = M \prod_{\chi} S(\chi')$, where the product is taken over all the non-trivial characters of $\mathrm{Gal}(H_f/K)$ (which includes χ) and M is a non-zero element of $\mathbf{C}_p$ (for an account of the archimedean analogue of this see [8], the argument goes over without change to the p-adic case). Hence $S(\chi) \neq 0$ and therefore, since it is well-known that $G(\chi) \neq 0$, $L_p(0,\chi) \neq 0$ as desired.

BIBLIOGRAPHY

[1] J. L. Boxall, *p*-adic Interpolation of Logarithmic Derivatives Associated to Certain Lubin-Tate Formal Groups, *Ann. Inst. Fourier*, Grenoble, 36, 3 (1986), to appear.

[2] J. L. Boxall, On p-adic L-functions Attached to Elliptic Curves with Complex Multiplication (to appear).

[3] A. Brumer, On the Units of Algebraic Number Fields, *Mathematika*, 14 (1967), 121-124.

[4] J. Coates and C. Goldstein, Some Remarks on the Main Conjecture for Elliptic Curves with Complex Multiplication, *Amer J. Math.*, 105 (1983), 337-366.

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

[6] J. Coates and A. Wiles, On *p*-adic L-functions and Elliptic Units, *J. Austral. Math. Soc.*, ser. A, 26 (1978), 1-25.

[7] R. Damerell, L-functions of Elliptic Curves with Complex Multiplication, *Acta Arith.*, 17 (1970), 287-301.

[8] R. Gillard and G. Robert, Groupes d'Unités Elliptiques, *Bull. Soc. Math. France*, 107 (1979), 305-317.

[9] C. Goldstein and N. Schappacher, Séries d'Eisenstein et Fonctions L de Courbes Elliptiques à Multiplication Complexe, *Crelle's J.*, 327 (1981), 184-218.

[10] K. Iwasawa, Lectures on *p*-adic L-functions, *Annals of Math. Studies*, 74 P.U.P. (1972).

[11] E. E. Kummer, Über eine allgemeine Eigenschaft der rationale Entwicklungs coefficienten einer bestimmten Gattung analysischer Functionen, *Crelle's* J., 41 (1851), 368-372, (= Collected Works vol. 1, pp. 358–362 Springer-Verlag (1975)).

[12] T. Kubota and H. W. Leopoldt, Eine *p*-adische Theorie der Zetawerte, *Crelle's* J., 214/215 (1964), 328-339.

[13] N. Katz, *p*-adic Interpolation of Real-Analytic Eisenstein Series, *Annals of Math.*, 104 (1976), 459-571.

[14] N. Katz, The Eisenstein Measure and *p*-adic Interpolation, *Amer. J. Math.*, 99 (1977), 238-311.

[15] N. Katz, Formal Groups and *p*-adic Interpolation, *Astérisque*, 41-42 (1977), 55-65.

[16] N. KATZ, Divisibilities, Congruences and Cartier Duality, *J. Fac. Sci. Univ. Tokyo*, Ser. 1A, 28 (1982), 667-678.
[17] S. LANG, *Elliptic Functions*, Addison Wesley (1973).
[18] H. W. LEOPOLDT, Eine p-adische Theorie der Zetawerte II, *Crelle's J.*, 274/275 (1975), 224-239.
[19] S. LICHTENBAUM, On p-adic L-functions Associated to Elliptic Curves, *Inventiones Math.*, 56 (1980), 19-55.
[20] J. LUBIN, One-Parameter Formal Lie Groups over p-adic Integer Rings, *Annals of Math.*, 80 (1964), 464-484.
[21] B. MAZUR and P. SWINNERTON-DYER, Arithmetic of Weil Curves, *Inventiones Math.*, 25 (1974), 1-61.
[22] B. MAZUR and A. WILES, Class fields of Abelian extensions of $\mathbf{Q}$, *Invent. Math.*, 76 (1984), 179-330.
[23] G. ROBERT, Unités Elliptiques, *Bull. Soc. Math. France*, Mémoire 36 (1973).
[24] K. RUBIN, Congruences for Special Values of L-functions of Elliptic Curves with Complex Multiplication, *Invent. Math.*, 71 (1983), 339-364.
[25] J.-P. SERRE, Formes Modulaires et Fonction Zêta p-adiques, in Springer *Lecture Notes in Math.*, 350 (1973), 191-268.
[26] J.-P. SERRE and J. TATE, Good Reduction of Abelian Varieties, *Annals of Math.*, 88 (1968), 492-517.
[27] E. DE SHALIT, Ph. D. Thesis, Princeton University (1984).
[28] J. TATE, p-divisible Groups, *Proc. Conf. on Local Fields*, Ed. T. Springer, Springer-Verlag (1967), 158-183.
[29] M. M. VISHIK and J. MANIN, p-adic Hecke Series of Imaginary Quadratic Fields, *Math. USSR Sbornik*, 24 (1974), 345-371.
[30] L. WASHINGTON, Introduction to Cyclotomic Fields, *Graduate Texts in Math.*, Springer-Verlag (1982).
[31] A. WEIL, *Elliptic Functions According to Eisenstein and Kronecker*, Springer-Verlag (1976).
[32] R. YAGER, On the Two-Variable p-adic L-function, *Annals of Math.*, 115 (1982), 411-449.
[33] R. YAGER, p-adic Measures on Galois Groups, *Inventiones Math.*, 76 (1984), 331-343.

Manuscrit reçu le 4 juin 1985.

John L. BOXALL,
Université de Caen
Département de Mathématiques
et de Mécanique
14032 CAEN Cedex
&
The University of Manchester
Institute of Science and Technology
P.O. Box 88
Manchester M60 1QD (G.B.).