Société Mathématique de France
Astérisque 61 (1979) p. 177-192

REPORT ON P-ADIC L-FUNCTIONS OVER TOTALLY REAL FIELDS

by

Kenneth A. Ribet

This report concerns known p-adic properties of values at negative integers of abelian L-functions over totally real fields. These properties were first established by P. Deligne and the author [5], using the theory of p-adic Hilbert modular forms. Recently, techniques found by P. Cassou-Noguès [2] and by D. Barsky [1], based on formulas of Shintani [7], have provided a totally new method for the p-adic study of L-values. The main object of this paper is to compare the congruence results obtained by the two methods

More precisely, the main theorem of [5] is a statement about the existence of p-adic measures with certain properties, or equivalently a theorem asserting generalized Kummer congruences for L-values. The main theorem of [2] establishes certain special congruences introduced (as axioms) by Coates in his study of p-adic L-functions [3]. These congruences are particular cases of the Kummer congruences. Here we shall explain how the congruences of Coates in fact generate *all* Kummer congruences, so that the main results given by the two methods are entirely equivalent. This comparison takes place in the second section of this paper, which follows a preliminary section on the rationality of L-values.

In the third section, we state some 2-adic divisibilities (and a *non*-divisibility) which follow from the modular form technique for studying L-values. These results, obtained in [5], form a complement to the main theorem on Kummer congruences. Some of these divisibilities may be deduced formally from the Kummer congruences, because of the existence of trivial zeros for L-functions attached to abelian characters. It appears, however, that the general divisibility cannot be so obtained. It might be interesting to reprove these divisibilities using the method based on Shintani's formulas.

In the fourth section, we restate the Kummer congruences for conductors which are divisible by p, in terms of measures on Galois groups. Then we review a construction of p-adic L-functions based on these measures. The construction is basically that given by Coates [3], except that the role of measures has been made explicit. In summary, it is the following: the p-adic L-functions, after multiplication by suitable "fudge factors," become the Mellin transforms (in the sense of Mazur) of our measures. In our discussion, we have indicated how one may eliminate constant consideration of the fudge factors by using the *pseudo-measures* recently introduced by Serre [6].

1. *Rationality properties of abelian L-values*

Let K be a totally real field, and set $r = [K:\mathbb{Q}]$. For each (non-zero) integral ideal (or "conductor") f of K, let G_f be the strict ray class group of K modulo f. Recall that G_f is obtained by dividing the set of prime-to-f integral ideals of K by the equivalence:

$$a \sim b \text{ if and only if } ab^{-1} = (\alpha) \text{ for some totally positive } \alpha \in 1 + fb^{-1} .$$

Let $\bar{K}$ be an algebraic closure for K. Class field theory interprets G_f as the Galois group of an abelian extension $K_f \subseteq \bar{K}$ of K, and the union $\bigcup_f K_f$ is the maximal abelian extension K^{ab} of K in $\bar{K}$.

Let f now be a conductor, and let v be an embedding $K \hookrightarrow \mathbb{R}$, i.e., a real place of K. Let $\alpha \in 1 + \mathfrak{f}$ be an element which is negative at v (i.e., $v(\alpha) < 0$) but positive at each real place of K different from v. The image σ_v in G_f of the ideal (α) is independent of the choice of α and has order 1 or 2. It is the (real) Frobenius element of G_f attached to v. It may also be described as the automorphism of G_f obtained by choosing an embedding $K_f \hookrightarrow \mathbb{C}$ compatible with v and applying complex conjugation.

For fixed v, as f varies, the elements $\sigma_v \in G_f$ form a compatible system in $G = \varprojlim G_f$. We again write σ_v for the element of G given by this compatible system. Each $\sigma_v \in G$ has order 2, and the subgroup H of G generated by the σ_v has order exactly 2^r. For each f, let H_f be the subgroup of G_f generated by the σ_v in G_f; this subgroup is the image of H in G_f.

If $\varepsilon: G_f \to \mathbb{C}$ is a complex-valued function mod f, we set as usual

$$L(s, \varepsilon) = \sum \varepsilon(x) Nx^{-s} , \tag{1.1}$$

the sum being over prime-to-f integral ideals x. (Here N is the norm function, and we view ε as a function on the set of prime-to-f ideals in the usual way.) While this sum need converge only for $\mathrm{Re}\, s > 1$, it is well known that the function $L(s, \varepsilon)$ may be analytically continued to a meromorphic function on $\mathbb{C}$, holomorphic for $s \neq 1$, with at worst a simple pole at $s = 1$. The continuation defines in particular values $L(1 - k, \varepsilon)$ for integral $k \geqslant 1$.

(1.2) THEOREM [7], [8]. *Suppose that the values of* ε *are rational numbers. Then* $L(1 - k, \varepsilon) \in \mathbb{Q}$ *for* $k \geqslant 1$.

For each $a \in G_f$, let $1_{a,f}$ be the characteristic function of a on G_f. The L-series $L(s, 1_{a,f})$ is the partial zeta function of the class a modulo f as considered by Siegel. The theorem asserts that the values of such partial zeta functions at negative integers (including 0) are rational. The formula

$$L(1 - k, \varepsilon) = \sum_{a \in G_f} L(1 - k, 1_{a,f}) \cdot \varepsilon(a)$$

shows for arbitrary $\varepsilon: G_f \to \mathbb{C}$ that the values $L(1 - k, \varepsilon)$ lie in the $\mathbb{Q}$-vector space spanned by the numbers $\varepsilon(a)$ in $\mathbb{C}$. It provides the *definition* of values $L(1-k, \varepsilon) \in V$ for any function on G_f with values in a $\mathbb{Q}$-vector space V.

We now consider certain identities which hold among these values. Let $\varepsilon: G_f \to V$ be given. For $a \in G_f$ we write ε_a for the function $x \longmapsto \varepsilon(ax)$, the "twist" of ε by a. For $c \in G$, we write ε_c for the twist of ε by the image of c in G_f. Similarly we define the twist of ε by a prime-to-f integral ideal d.

(1.3) PROPOSITION. *Assume that* $K \neq \mathbb{Q}$ *or that* f *is non-trivial. For each real place* v *of* K *and all* $k \geq 1$, *we have* $L(1-k, \varepsilon_{\sigma_v}) = (-1)^k L(1-k, \varepsilon)$.

The proposition is proved by reduction to the case where ε is a primitive character with values in $\mathbb{C}^*$. It follows in this case from the functional equation for $L(s, \varepsilon)$ (trivial zeros). Note that in the excluded case the proposition would be false for $k = 1$, since the Riemann zeta function does not vanish at 0.

Now let $f' \subset f$ be two conductors. Suppose that d is a divisor of f' which is prime to f. Then f divides the quotient $f'd^{-1}$, so that there is a canonical map $G_{f'd^{-1}} \to G_f$. Let us write ε_d^* for the composite of this canonical map with the twist ε_d of ε by d. The function ε_d^* is thus a function mod $f'd^{-1}$.

(1.4) PROPOSITION. *For* $k \geq 1$ *we have*

$$L(1-k, \varepsilon) = \sum_d L(1-k, \varepsilon_d^*) Nd^{k-1},$$

where the sum runs over those divisors d *of* f' *which are prime to* f.

To prove this proposition, it suffices to treat the case $V = \mathbb{C}$. There we decompose the sum (1.1) according to the greatest common divisor d of x and f'. The asserted identity then falls out immediately.

The simplest, and most familiar, case of the identity (1.4) occurs when f and f' have the same prime factors. Then the sum has only one term, corresponding to $d = 1$, and the identity states that $L(1-k, \varepsilon)$ has the same value when we regard ε as a function modulo f' as when we regard it as a function modulo f.

2. *Congruences for L-values*

Let p be a prime number, fixed in what follows. Let $N : G \to \mathbb{Z}_p^*$ be the p-adic norm character. This map is characterized by each of the following:

(i) The map N is the "Tate" character describing the action of $G = \mathrm{Gal}(K^{ab}/K)$ on the p-power roots of unity in K^{ab}.

(ii) The map N factors through the quotient $G_{p^\infty} = \varprojlim G_{p^n}$ of G and coincides with the standard norm map on the dense subset of G_{p^∞} consisting of the prime-to-p integral ideals of K.

In connection with (ii), we note that for $n \geqslant 0$ the map

$$N \bmod p^n ; \; G \xrightarrow{N} \mathbb{Z}_p^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$$

already factors across the quotient G_{p^n} of G. Also, we have $N_{\sigma_v} = -1$ for each real place v of K.

Let f be a conductor, and let $\varepsilon : G_f \to V$ take values in a $\mathbb{Q}_p$-vector space. For $c \in G$ we set

$$\Delta_c(1 - k, \varepsilon) = L(1 - k, \varepsilon) - Nc^k L(1 - k, \varepsilon_c) \in V$$

for $k \geqslant 1$. These ε_c are the *twisted L-values* attached to ε. If ε is a *character* with values in an extension field of $\mathbb{Q}_p$, then we have

$$\Delta_c(1 - k, \varepsilon) = \{1 - \varepsilon(c)Nc^k\} L(1 - k, \varepsilon) :$$

the twisted L-values are the usual L-values corrected by a "fudge factor" depending on c.

Now let $(\varepsilon_k, k \geqslant 1)$ be a sequence of $\mathbb{Q}_p$-valued functions on G_f, *only finitely many of which are non-zero.* The Kummer congruences mentioned in the Introduction are given by

(2.1) THEOREM [5]. *Assume that we have*

$$\sum_{k\geq 1} \varepsilon_k(x) Nx^{k-1} \in \mathbb{Z}_p$$

for each prime-to-f integral ideal x . *Then for all* $c \in G$ *we have*

$$\sum_{k\geq 1} \Delta_c(1-k, \varepsilon_k) \in \mathbb{Z}_p \ .$$

We note immediately the following *variants* of (2.1):

1. By linearity, we may replace $\mathbb{Z}_p$ by $p^n\mathbb{Z}_p$ for any $n \in \mathbb{Z}$, in the statement of (2.1). Hence (2.1) may be paraphrased: any *congruence* satisfied by a finite sum $\sum \varepsilon_k N^{k-1}$ is again satisfied by the corresponding sum of twisted L-values.

2. We may replace $\mathbb{Z}_p$ by any free $\mathbb{Z}_p$-module R , replacing $\mathbb{Q}_p$ by $E = R \otimes \mathbb{Q}_p$. This applies for example if E is a finite extension of $\mathbb{Q}_p$ and R is its ring of integers.

3. We may replace c by an *integral ideal* d which is prime to pf . The conclusion of (2.1) for a given c is equivalent to the corresponding statement for a given d provided that c and d have the same images in G_f and have norms which are sufficiently p-adically close.

We now turn to the congruences of Coates [3]. We restate them slightly, to make evident that they are special cases of the Kummer congruences (2.1):

A. *For all* $\varepsilon: G_f \to \mathbb{Z}_p$ *and* $k \geq 1$, *we have* $\Delta_c(1-k, \varepsilon) \in \mathbb{Z}_p$ *for all* $c \in G$.

B. *Let* f *be divisible by* p^n $(n \geq 0)$, *and let* $k \geq 1$ *be given. Suppose that* $\eta: G_f \to \mathbb{Z}_p$ *is such that* $\eta \equiv N^{k-1} \bmod p^n$, *the two functions being considered as functions on the space of prime-to-f integral ideals. Then for all* $\varepsilon: G_f \to \mathbb{Z}_p$ *we have*

$$\Delta_c(1-k, \varepsilon) \equiv \Delta_c(0, \varepsilon\eta) \bmod p^n \ .$$

[Note that, in *B*, the function η exists because $N \bmod p^n$ may be viewed as a function on G_{p^n} . Assuming *A*, the assertion *B* is independent of the choice of η .]

(2.2) THEOREM. *Statements* A *and* B *imply* (2.1).

Proof. We first condider the case where f is divisible for all primes dividing p. For $n \geqslant 0$ we have the right to replace f by fp^n in (2.1), replacing ε_k by their composites with the map $G_{fp^n} \to G_f$: The replacement does not change the hypothesis of (2.1), and in light of (1.4) it does not change the conclusion either. Make this replacement, choosing n so that all ε_k take value in $p^{-n}Z_p$. For each $k \geqslant 1$, let η_k be such that $\eta_k \equiv N^{k-1} \bmod p^n$. The function

$$\varepsilon = \sum \varepsilon_k \eta_k$$

is $\mathbb{Z}_p$-valued according to the hypothesis to (2.1). Hence, by *A*, we have $\Delta_c(0, \varepsilon) \in \mathbb{Z}_p$. But by *B* we have

$$\Delta_c(0, \varepsilon_k \eta_k) \equiv \Delta_c(1 - k, \varepsilon_k) \quad \bmod \mathbb{Z}_p$$

for each k. Since $\Delta_c(0, \varepsilon) = \sum \Delta_c(0, \varepsilon_k \eta_k)$, this gives the conclusion to (2.1).

We now treat the remaining case, where f is *not* divisible by all primes over p. Each class in G_f is represented by ideals whose norms are arbitrarily highly divisible by p, so that the hypothesis to (2.1) implies that ε_1 takes values in $\mathbb{Z}_p$. Of course, if *all* ε_k are $\mathbb{Z}_p$-valued, then the conclusion to (2.1) is a consequence of *A*. Arguing inductively, we shall assume that (2.1) is known if all ε_k take values in $p^{-n}\mathbb{Z}_p$ but that we are in fact given functions ε_k with values in $p^{-n-1}\mathbb{Z}_p$.

Let $f' = fp$, and decompose each value $L(1 - k, \varepsilon_k)$ as in (1.4). The quantity to be proved integral in (2.1) then breaks up as a sum of quantities $\sum_k \Delta_c(1 - k, \varepsilon^*_{k,d})Nd^{k-1}$, one for each divisor d of f' which is prime to f. It suffices to prove that each such quantity is integral. Fix d, and for each k set $\alpha_k = \varepsilon^*_{k,d}\, Nd^{k-1}$; the problem is then to obtain the conclusion of (2.1) with the ε_k replaced by the α_k. Now for each x prime to $f'd^{-1}$, we have

$$\sum_k \alpha_k(x)Nx^{k-1} = \sum_k \varepsilon_k(dx)N(dx)^{k-1},$$

so that the hypothesis of (2.1) for the α_k is just a special case of the same hypothesis for the ε_k . If $d = 1$, then $\mathfrak{f} = \mathfrak{f}\mathfrak{p}$ is divisible by all primes over p , so we have already obtained the conclusion of (2.1) for the α_k . If $d \neq 1$, then clearly Nd is divisible by p , so that each α_k takes values in $p^{-n}\mathbb{Z}_p$. We again have the desired integrality by induction.

3. *2-adic properties of* L-*values, and "parity"*

In this section we state a strengthening of (2.1) for $p = 2$ in the situation where the functions ε_k satisfy certain parity conditions.

Let $\mathfrak{f}$ be a conductor. A function ε on $G_{\mathfrak{f}}$ with values in a $\mathbb{Q}$-vector space V is said to be *odd* (resp. *even*) if $\varepsilon_{\sigma_v} = -\varepsilon$ (resp. $\varepsilon_{\sigma_v} = \varepsilon$) for each real place v of K . (Here the σ_v are the real Frobenius elements of §1.) Let k be an integer. We say that ε has parity $(-1)^k$ if k is odd and ε is odd or if k is even and ε is even. We shall be considering functions ε_k as in (2.1) where each ε_k has parity $(-1)^k$. Before doing this, we distinguish an *exceptional case*. This is the case where each of the following three conditions is satisfied:

(i) The conductor $\mathfrak{f}$ is the trivial ideal (1).

(ii) All units of K have norm $+1$.

(iii) The extension L of K obtained by extracting the square roots of all totally positive units of K is *quadratic* over K .

[When (ii) is satisfied, (iii) means that there are units of K of all possible signatures which are compatible with (ii).]

Finally, suppose that $\varepsilon\colon G_{\mathfrak{f}} \to \mathbb{Z}_2$ is either even or odd. Then the reduction

$$\bar{\varepsilon}\colon G_{\mathfrak{f}} \xrightarrow{\varepsilon} \mathbb{Z}_2 \longrightarrow (\mathbb{Z}/2\mathbb{Z})$$

is invariant under the subgroup $H_{\mathfrak{f}}$ of $G_{\mathfrak{f}}$ generated by the σ_v , so that the sum

$$\sum_{g \in G_{\mathfrak{f}}/H_{\mathfrak{f}}} \bar{\varepsilon}(g) \in \mathbb{Z}/2\mathbb{Z}$$

is well defined. We let $\delta(\varepsilon)$ denote this sum.

(3.1) THEOREM [5]. *Let* ε_k $(k \geqslant 1)$ *be given as in* (2.1). *Assume that each* ε_k *has parity* $(-1)^k$ *and that* $p = 2$. *Then:*

(a) *For all* $c \in G$ *we have*

$$\Delta_c \overset{\text{def.}}{=} \sum_{k \geqslant 1} \Delta_c(1 - k, c_k) \in 2^{r-1}\mathbb{Z}_2,$$

(b) *In the non-exceptional case, we have* $\Delta_c \in 2^r\mathbb{Z}_2$.

(c) *In the exceptional case, we have* $\Delta_c \in 2^r\mathbb{Z}_2$ *provided that either* $c \in Gal(K^{ab}/L)$ *or* $\delta(\varepsilon_1) = 0$.

[Note that in the exceptional case the function ε_1 is $\mathbb{Z}_2$-valued because the conductor $f = (1)$ is not divisible by each prime dividing 2, as in the proof of (2.2).]

(3.2) THEOREM [5]. *Suppose, in the exceptional case, that* $\delta(\varepsilon_1) = 1$ *and that* $c \notin Gal(K^{ab}/L)$. *Then* Δ_c *is exactly divisible by* 2^{r-1}.

In connection with these theorems, we now explain why the case where each ε_k has parity $(-1)^k$ is a central one. As in §1, let H be the subgroup of G generated by the real Frobenius elements σ_v. Let $N\colon H \to \{\pm 1\}$ be the homomorphism such that $N\sigma_v = -1$ for each v; it is the restriction to H of the p-adic norm character $N\colon G \to \mathbb{Z}_p$ for any prime p.

Suppose that ε is a function on G_f with values in a $\mathbb{Q}$-vector space. Write

$$\varepsilon^+ = \frac{1}{\#H} \sum_{c \in H} \varepsilon_c,$$

$$\varepsilon^- = \frac{1}{\#H} \sum_{c \in H} Nc \cdot \varepsilon_c;$$

these two functions are respectively even and odd. (As we have remarked in §1, one knows in fact that $\#H = 2^r$.)

(3.3) PROPOSITION. *Suppose that either* K *is different from the rational field or that* f *is non-trivial.*

(1) *For* $k \geqslant 1$ *and* $c \in H$ *we have* $L(1 - k, \varepsilon_c) = Nc^k L(1 - k, \varepsilon)$,

(2) *We have*

$$L(1-k,\varepsilon)=\begin{cases}L(1-k,\varepsilon^{+}) & \text{if } k \text{ is even}\\ \\ L(1-k,\varepsilon^{-}) & \text{if } k \text{ is odd,}\end{cases}$$

Proof. The first statement is a variant of (1.3). The second follows directly from the first and the definitions of ε^{-}, ε^{+}.

Statement (2) gives a simple expression for an arbitrary L-value in terms of an L-value for a function "with parity." Using it, one shows easily that (2.1), when $p = 2$, is a *consequence* of (3.1). Conversely, given (2.1), the divisibility statement (3.1) may be reinterpreted in terms of divisibilities of values $\Delta_c(0,\varepsilon)$ for *arbitrary* functions $\varepsilon: G_f \to \mathbb{Z}_2$.

4. p-*adic* L-*functions and* p-*adic measures*

Let p be a prime number. In this section we shall outline the construction of p-adic measures on certain Galois groups with the aim of relating our Kummer congruence (2.1) to the theory of p-adic L-functions attached to abelian characters over K.

Let f be a conductor which is divisible by all primes of K dividing p. In this section, we modify our previous notation and let G be the Galois group $G_{fp^\infty} = \varprojlim G_{fp^n}$. The group *previously* denoted by G will now be referred to without abbreviation as $\mathrm{Gal}(K^{ab}/K)$. We shall reformulate in terms of measures on G all Kummer congruences modulo the conductors fp^n $(n \geq 0)$.

For each locally constant function $\varepsilon: G \to \mathbb{Q}$, quantities $L(1-k,\varepsilon) \in \mathbb{Q}$ are defined for $k \geq 1$. Namely, any such ε is (for sufficiently large n) a map $G_{fp^n} \xrightarrow{\varepsilon_n} \mathbb{Q}$, and the numbers $L(1-k,\varepsilon_n)$ attached to this map as in §1 are independent of the choice of n because of (1.4). For fixed k, the association $\varepsilon \mapsto L(1-k,\varepsilon)$ is thus a distribution on G with values in $\mathbb{Q}$.

For each locally constant $\varepsilon: G \to \mathbb{Q}_p$ and each $c \in \mathrm{Gal}(K^{ab}/K)$, we define

$$\Delta_c(1-k,\varepsilon) = L(1-k,\varepsilon) - Nc^k L(1-k,\varepsilon_c) \in \mathbb{Q}_p$$

as in §2. Since $N\colon \mathrm{Gal}(K^{ab}/K) \to \mathbb{Z}_p^*$ may be viewed as a function on G, for given ε and k a quantity $\Delta_c(1-k, \varepsilon)$ is well defined for c in G.

For later use, we recall the standard factorization $N = \langle\ \rangle\omega$ of the norm character on G as the product of a character $x \longmapsto \langle x\rangle$ with values in $1 + 2p\mathbb{Z}_p \subseteq \mathbb{Z}_p^*$ and a $\mathbb{Z}_p^*$-valued character of finite order ω, the Teichmüller character. We let $\Gamma \subset \mathbb{Z}_p^*$ be the image of $\langle\ \rangle$; it is (non-canonically) isomorphic to $\mathbb{Z}_p$. The extension of K cut out by the character $\langle\ \rangle$ is the cyclotomic $\mathbb{Z}_p$-extension of K.

Also, we let $A \subseteq G$ be the kernel of $\langle\ \rangle$; it is finite if and only if the Leopoldt conjecture is true for K and p.

(4.1) THEOREM. *For each* $c \in G$, *the distribution* $\varepsilon \longmapsto \Delta_c(0, \varepsilon)$ *is a measure* μ_c *on* G *with values in* $\mathbb{Z}_p$. *For* $k \geqslant 1$, *the measure* $N^{k-1}\mu_c$ *is the map* $\varepsilon \mapsto \Delta_c(1-k, \varepsilon)$.

Proof. The first statement asserts that if a locally constant function ε on G is $\mathbb{Z}_p$-valued, then $\Delta_c(0, \varepsilon)$ lies in $\mathbb{Z}_p$. This is a special case of (2.1), and indeed is contained in congruence *A* of §2. To check the second statement, it suffices to show for $k \geqslant 1$ and $n \geqslant 1$ that

$$\int \varepsilon N^{k-1}\, d\mu_c \equiv \Delta_c(1-k, \varepsilon) \bmod p^n\, \mathbb{Z}_p$$

for each locally constant $\varepsilon\colon G \to \mathbb{Z}_p$. For this, let $\eta\colon G \to \mathbb{Z}_p$ be a locally constant function such that $\eta \equiv N^{k-1} \bmod p^n$. By congruence *B* of §2, we have

$$\Delta_c(1-k, \varepsilon) \equiv \Delta_c(0, \varepsilon\eta) \mod p^n\mathbb{Z}_p.$$

On the other hand, because μ_c is a measure, we have

$$\Delta_c(0, \varepsilon\eta) = \int \varepsilon\eta\, d\mu_c \equiv \int \varepsilon N^{k-1} d\mu_c \mod p^n\mathbb{Z}_p.$$

This completes the proof.

Remark. Conversely, we recover the Kummer congruences mod fp^n $(n \geqslant 0)$ from the measures μ_c as follows: if $\sum \varepsilon_k N^{k-1}$ is $\mathbb{Z}_p$-valued, then we have

$$\sum \Delta_c(1-k, \varepsilon_k) = \int \sum \varepsilon_k N^{k-1} d\mu_c \in \mathbb{Z}_p.$$

Since our proof of (4.1) uses only congruences A and B of §2, we find once again that A and B imply the Kummer congruences for any conductor divisible by all primes above p. The proof of this fact provided by the above arguments is essentially the same as that given in §2.

Following [6], it is convenient to renormalize so as to replace $k-1$ by k. Namely, for $c \in G$, let $\lambda_c = N^{-1}\mu_c$. Then λ_c is a measure on G with the property that

$$\int \varepsilon N^k \, d\lambda_c = \Delta_c(1-k, \varepsilon)$$

for $k \geqslant 1$ and ε locally constant (cf. [6, 3.5]).

In the language of [6], the measures λ_c define a *pseudo-measure* λ on G. For each non-trivial continuous character ψ on G with values in the completion $\mathbb{C}_p$ of the algebraic closure of $\mathbb{Q}_p$, an integral

$$\int \psi d\lambda = \frac{\int \psi d\lambda_c}{1-\psi(c)} \in \mathbb{C}_p$$

is defined independently of c. When ψ is a character of finite order, we have in particular $\int \psi N^k \, d\lambda = L(1-k, \psi)$.

(4.3) Suppose that Leopoldt's conjecture is true for K and p, i.e., that the group $A = \mathrm{Ker}\langle\ \rangle$ is finite. Then by [6, 1.15], λ may be uniquely written as the sum of a $\mathbb{Z}_p$-valued measure μ on G and some $\mathbb{Z}_p$-multiple of a certain "standard" pseudo-measure on G obtianed from Haar measure on A. On the other hand, if Leopoldt's conjecture is false for K and p, then [6, 1.15] states that λ is already a measure. Write $\mu = \lambda$ in this case. Then in both cases we have at least $\int \psi \, d\lambda = \int \psi \, d\mu$ for all characters ψ which are non-trivial on A [6, 1.17].

Now let $H \subseteq G$ be the subgroup of G generated by the real Frobenius elements of G (i.e., the images in G of the real Frobenius elements of $\mathrm{Gal}(K^{ab}/K)$).

(4.4) THEOREM. *Let* $\phi: G \to \mathbb{Z}_p$ *be a continuous function which is even in the sense that it is invariant under* H. *Then for all* $c \in G$ *we have* $\int \phi \, d\lambda_c \in 2^r\mathbb{Z}_p$.

Proof. There is no new assertion if p is odd. If $p = 2$, the result follows immediately from divisibility (b) of (3.1).

Remark. Using (3.3), one may show *a priori* from (4.1) that $\int \phi \, d\lambda_c$ is divisible in $\mathbb{Z}_p$ by the order of H when ϕ is even. This order divides 2^r, and it is equal to 2^r whenever $p = 2$ and Leopoldt's conjecture is true for K and the prime 2. Hence (4.4) asserts the truth of a *consequence* of Leopoldt's conjecture.

(4.5) COROLLARY. *Let* μ *be the measure on* G *introduced in* (4.3). *For all even* $\phi: G \to \mathbb{Z}_p$, we have $\int \phi \, d\mu \in 2^r \mathbb{Z}_p$.

Proof. The divisibility (4.4) asserts that the pseudo-measure on G/H obtained from λ and the projection $G \to G/H$ is divisible by 2^r. The corollary then follows from the uniqueness of the decomposition [6, 1.15].

We close now with remarks on the construction of the p-adic L-function $L_p(s, \varepsilon)$ attached to an even continuous character ε of finite order on G. Let E be the finite extension of $\mathbb{Q}_p$ generated by the values of ε, and let R be the integer ring of E. By definition $L_p(s, \varepsilon)$ is the continuous function (of s) on $\mathbb{Z}_p - \{1\}$ with values in E such that $L_p(1 - k, \varepsilon) = L(1 - k, \varepsilon\omega^{-k})$ for $k \geq 1$. The point is to show that $L_p(s, \varepsilon)$ exists, and to derive various "analyticity" properties for it.

For the existence, choose an element c of G such that one of $\varepsilon(c)$, c is different from 1. The expression

$$\text{(4.6)} \qquad \frac{\int \langle x \rangle^{1-s} \varepsilon(x) \, d\lambda_c(x)}{1 - \varepsilon(c) \langle c \rangle^{1-s}}$$

then represents a continuous funciton of s having the defining property of $L_p(s, \varepsilon)$. Alternately, $L_p(s, \varepsilon)$ is simply the integral of $\varepsilon \langle \ \rangle^{1-s}$ against the pseudo-measure λ.

The analyticity properties result form the well-known connection between R-valued measures on $\mathbb{Z}_p$ and elements of the power series ring $R[[T]]$, cf. [6, 1.7].

The essential fact for us is a resulting *integral formula*. Choosing a splitting of the projection $G \to \Gamma$, so that G may be viewed as a product $\Gamma \times A$. Also, let $\gamma \in \Gamma$ be a topological generator of Γ over $\mathbb{Z}_p$. If $\alpha: \Gamma \xrightarrow{\sim} \mathbb{Z}_p$ is the resulting isomorphism, we have $x = \gamma^{\alpha(x)}$ for $x \in \Gamma$. We write simply α for the composite of α with the projection $G \to \Gamma$.

Let ψ be a continuous character on G with values in $\mathbb{C}_p^*$. It is the product of a character ψ_A on G which is trivial on Γ and the character $x \mapsto u^{\alpha(x)}$, where $u = \psi(\gamma)$. For $n \geqslant 0$, let a_n be the integral

$$\int_G \psi_A(x) \binom{\alpha(x)}{n} d\mu(x) \in R ,$$

where $\binom{\alpha(x)}{n}$ is the n^{th} binomial function on $\mathbb{Z}_p$, viewed via α as a function on G. Then, by the binomial theorem, we have

$$\int \psi d\mu = \sum_{n \geqslant 0}^{\infty} a_n (u-1)^n , \tag{4.7}$$

cf. [6, 1.9].

One uses this formula to prove results of *Iwasawa analyticity* for $L_p(s, \varepsilon)$. Namely, let us say that function $\psi: \mathbb{Z}_p \to R$ is Iwasawa analytic if there is a power series $F \in R[[T]]$ such that $F(\gamma^{1-s} - 1) = \phi(s)$. [The power series is unique if it exists, and the property of being analytic in this sense is independent of the choice of the generator γ of Γ.] Here are the nain facts concerning $L_p(s, \varepsilon)$:

(4.8) *For each* c, *both the numerator and the denominator in* (4.6) *are Iwasawa analytic function on* $\mathbb{Z}_p$. *The power series representing the numerator is divisible by* 2^r.

(4.9) *If* ε *is non-trivial on* A, *then* $L_p(s, \varepsilon)$ *extends to an Iwasawa analytic function on* $\mathbb{Z}_p$, *and the power series* F_ε *which represents it is divisible by* 2^r.

(4.10) *If* ε *is non-trivial on* A, *but if* $\theta: G \to \mathbb{C}_p^*$ *is a finite character which is trivial on* A, *then* $F_{\theta\varepsilon}(T) = F_\varepsilon(\zeta(1+T) - 1)$, *where* ζ *is the* *p-power root of unity* $\theta(\gamma)$.

Sketches of the proofs. The assertion relative to the denominator of (4.6) is immediate from the definition of the denominator. The Iwasawa analyticity of the numerator follows from (4.7), where we take $\psi = \langle\ \rangle^{1-s}$ and $\mu = \varepsilon\lambda_c$. The divisibility of the coefficients of the power series representing the numerator is a consequence of (4.4) and the hypothesis that ε is an even character. (It is worth noting, in passing, that when ε is a character which is *not* even, the definition of $L_p(s, \varepsilon)$ implies that $L_p(s, \varepsilon)$ is identically 0 .)

The statements in (4.9) may be deduced from (4.8) by an argument involving unique factorization in $R[[T]]$ (cf. [4], 6.5). A more direct approach is to use the expression

$$L_p(s, \varepsilon) = \int \varepsilon\langle\ \rangle^{1-s}d\mu ,$$

valid when ε is non-trivial on A , for $L_p(s, \varepsilon)$ in terms of the measure μ of (4.3). The divisibility of F_ε by 2^r results from (4.5).

Finally, (4.10) is an easy consequence of the integration formula (4.7); we have

$$\begin{aligned} L_p(s, \varepsilon\theta) &= \int (\langle\ \rangle^{1-s}\theta)\varepsilon d\lambda \\ &= F_\varepsilon(\gamma^{1-s}\theta(\gamma) - 1) . \end{aligned}$$

BIBLIOGRAPHY

[1] D. BARSKY - Fonctions zêta p-adiques d'une classe de rayon des corps de nombres totalement réels. Preprint.

[2] P. CASSOU-NOGUÈS - Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. Preprint.

[3] J. COATES - p-adic L-functions and Iwasawa's theory. In: Algebraic number fields, A. Fröhlich, ed. New York and London: Academic Press 1977.

[4] J. COATES and S. LICHTENBAUM - On ℓ-adic zeta functions. Ann. of Math *98*, 498-550 (1973).

[5] P. DELIGNE and K. RIBET - Values of abelian L-functions at negative integers. To appear.

[6] J.-P. SERRE - Sur le résidu de la fonction zêta p-adique d'un corps de nombres; C.R. Acad. Sc. Paris *287*, 183-188 (1978).

[7] T. SHINTANI - On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. J. Fac. Sci. Univ. Tokyo, Sec. IA *23*, 393-417 (1976).

[8] C.L. SIEGEL - Über die Fourierschen Koeffizienten von Modulformen. Göttingen Nach. *3*, 15-56 (1970).

Kenneth A. Ribet
Mathematics Dept.
U.C. Berkeley
BERKELEY, CA. 94720
(U.S.A)