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 \( \mathbb{G}_f \) be the strict ray class group of \( K \) modulo \( f \). Recall that \( \mathbb{G}_f \) is obtained by dividing the set of prime-to-\( f \) integral ideals of \( K \) by the equivalence:

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

Let \( \mathbb{F} \) be an algebraic closure for \( K \). Class field theory interprets \( \mathbb{G}_f \) as the Galois group of an abelian extension \( K_f \subseteq \mathbb{F} \) of \( K \), and the union \( \bigcup_f K_f \) is the maximal abelian extension \( K^{ab} \) of \( K \) in \( \mathbb{F} \).

Let \( f \) now be a conductor, and let \( v \) be an embedding \( K \rightarrow \mathbb{R} \), i.e., a real
place of \( K \), let \( a \in 1 + f \) be an element which is negative at \( v \) (i.e., \( v(a) < 0 \)) but positive at each real place of \( K \) different from \( v \). The image \( \sigma_v \) of the ideal \((a)\) is independent of the choice of \( a \) 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 \( G = \lim_{\leftarrow} G_f \). We again write \( \sigma_v \) 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 \( \sigma_v \) has order exactly \( 2^r \). For each \( f \), let \( H_f \) be the subgroup of \( G_f \) generated by the \( \sigma_v \) 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

\[
L(s, \varepsilon) = \sum \varepsilon(x)x^{-s},
\]

the sum being over prime-to-f integral ideals \( x \). (Here \( H \) is the norm function, and we view \( \varepsilon \) as a function on the set of prime-to-f ideals in the usual way.)

While this sum need converge only for \( \Re s > 1 \), 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 \( k \geq 1 \).

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

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

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

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 \( \epsilon(a) \) in \( \mathbb{C} \). It provides the definition of values \( L(1 - k, \epsilon) \in V \) 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 \( \epsilon: G_f \to V \) be given. For \( a \in G_f \) we write \( \epsilon_a \) for the function \( x \mapsto \epsilon(ax) \), the "twist" of \( \epsilon \) by \( a \). For \( c \in G \), we write \( \epsilon_c \) for the twist of \( \epsilon \) by the image of \( c \) in \( G_f \). Similarly we define the twist of \( \epsilon \) 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 \( k \gg 1 \), we have \( L(1 - k, \epsilon_v) = (-1)^k L(1 - k, \epsilon) \).

The proposition is proved by reduction to the case where \( \epsilon \) is a primitive character with values in \( \mathbb{C}^* \). It follows in this case from the functional equation for \( L(s, \epsilon) \) (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 \( f' \mid f \) 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 \( \epsilon_d^* \) for the composite of this canonical map with the twist \( \epsilon_d \) of \( \epsilon \) by \( d \). The function \( \epsilon_d^* \) is thus a function mod \( f' d^{-1} \).

(1.4) PROPOSITION. For \( k \gg 1 \) we have

\[
L(1 - k, \epsilon) = \sum_d L(1 - k, \epsilon_d^*) \mu d^{-1},
\]

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 \( c \) 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 \( L(1 - k, \epsilon) \) has the same value when we
regard $\epsilon$ 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 $N: G \to \mathbb{Z}_p^\times$ be the $p$-adic norm character. This map is characterized by each of the following:

(1) The map $N$ is the "Tate" character describing the action of

$G = \text{Gal}(K^{ab}/K)$ on the $p$-power roots of unity in $K^{ab}$.

(11) The map $N$ factors through the quotient $G = \lim_{p \to \infty} G_p$ 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 (11), we note that for $n \gg 0$ the map

$$N \mod p^n: G \to \mathbb{Z}^\times_p \to (\mathbb{Z}/p^n\mathbb{Z})^\times$$

already factors across the quotient $G_p^n$ of $G$. Also, we have $N_v = -1$ for each real place $v$ of $K$.

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

$$\Delta_c(l - k, \epsilon) = L(l - k, \epsilon) - N_c^k L(l - k, \epsilon_c) \in V$$

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

$$\Delta_c(l - k, \epsilon) = (l - \epsilon(c) N_c^k) L(l - k, \epsilon);$$

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

Now let $(c_k, k \gg 1)$ 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

\[ \sum_{k \geq 1} \varepsilon_k(x)\mu^{k-1} \in \mathbb{Z}_p \]

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 \( \sum \varepsilon_k^{k-1} \) 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 \( \mathcal{R} \), replacing \( \mathbb{Q}_p \) by \( H = \mathcal{R} \otimes \mathbb{Q}_p \). This applies for example if \( \mathcal{R} \) is a finite extension of \( \mathbb{Q}_p \) and \( \mathcal{R} \) 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 \( \mathcal{O}_\mathcal{A} \) 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 \( \varepsilon: \mathcal{Q}_F \rightarrow \mathcal{O}_\mathcal{A} \) 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 \( \eta: \mathcal{Q}_F \rightarrow \mathcal{O}_\mathcal{A} \) is such that \( \eta \equiv \nu^{k-1} \mod p^n \), the two functions being considered as functions on the space of prime-to-f integral ideals. Then for all \( \varepsilon: \mathcal{Q}_F \rightarrow \mathcal{O}_\mathcal{A} \) we have

\[ \Delta_c(1 - k, \varepsilon) \equiv \Delta_c(0, \varepsilon\eta) \mod p^n. \]

[Note that, in \( E \), the function \( \eta \) exists because \( \eta \mod p^n \) may be viewed as a function on \( \mathcal{O}_\mathcal{A} \). Assuming \( A \), the assertion \( B \) is independent of the choice of \( \eta \).]
(2.2) THEOREM. Statemente A and B imply (2.1).

Proof. We first consider the case where $f$ is divisible for all primes dividing $p$. For $n \geq 0$ we have the right to replace $f$ by $fp^n$ in (2.1), replacing $e_k$ by their composites with the map $G_p \to G_p$. The replacement does not change the hypothesis of (2.1), and in light of (1.1) it does not change the conclusion either.

Make this replacement, choosing $n$ so that all $e_k$ take values in $p^{-n} \mathbb{Z}_p$. For each $k \geq 1$, let $n_k$ be such that $n_k = n^{k-1} \mod p^n$. The function

$$e = \sum_k e_k n_k$$

is $\mathbb{Z}_p$-valued according to the hypothesis to (2.1). Hence, by $A$, we have

$$\Delta_c(0, e) \in \mathbb{Z}_p.$$ But by $B$ we have

$$\Delta_c(0, e_{\bar{k}n_k}) = \Delta_c(1 - k, e_k) \mod \mathbb{Z}_p$$

for each $k$. Since $\Delta_c(0, e) = \prod_k \Delta_c(0, e_{\bar{k}n_k})$, 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 $G_p$ is represented by ideals whose norms are arbitrarily highly divisible by $p$, so that the hypothesis to (2.1) implies that $e$ takes values in $\mathbb{Z}_p$. Of course, if all $e_k$ 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 $e_k$ take values in $p^{-n} \mathbb{Z}_p$ but that we are in fact given functions $e_k$ with values in $p^{-n-1} \mathbb{Z}_p$.

Let $f' = fp$, and decompose each value $L(1 - k, e_k)$ as in (1.4). The quantity to be proved integral in (2.1) then breaks up as a sum of quantities

$$\sum_k \Delta_c(1 - k, e_k) N^{x^k}$$

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 $a_k = e_k \equiv N^{x^k} \mod d$; the problem is then to obtain the conclusion of (2.1) with the $e_k$ replaced by the $a_k$. Now for each $x$ prime to $f' d^{-1}$, we have

$$\sum_k a_k(x) N^{x^k} = \sum_k e_k(x) N^{x^k} d^{-1},$$

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

3. $3$-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 $\varepsilon_k$ satisfy certain parity conditions.

Let $f$ be a conductor. A function $\varepsilon$ on $G_f$ with values in a $\mathbb{Q}$-vector space $V$ is said to be odd (resp. even) if $c_{\varphi_V} = -c$ (resp. $c_{\varphi_V} = c$) for each real place $\varphi$ of $K$. (Here the $c_{\varphi_V}$ are the real Frobenius elements of $\varphi_V$.)

Let $k$ be an integer. We say that $\varepsilon$ has parity $(-1)^k$ if $k$ is odd and $\varepsilon$ is odd or if $k$ is even and $\varepsilon$ is even. We shall be considering functions $\varepsilon_k$ as in (2.1) where each $\varepsilon_k$ 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 $f$ 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 $\varepsilon : G_f \rightarrow \mathbb{Z}_2$ is either even or odd. Then the reduction

$$\tilde{\varepsilon} : G_f \rightarrow \mathbb{Z}_2 \rightarrow (\mathbb{Z}/2\mathbb{Z})$$

is invariant under the subgroup $H_f$ of $G_f$ generated by the $c_{\varphi_V}$, so that the sum

$$\sum_{g \in G_f/H_f} \tilde{\varepsilon}(g) \in \mathbb{Z}/2\mathbb{Z}$$

is well-defined. We let $d(\varepsilon)$ denote this sum.
(3.1) THEOREM [5]. Let \( \epsilon_k \) \((k \gg 1)\) be given as in (2.1). Assume that each \( \epsilon_k \) has parity \((-1)^k\) and that \( p = 2 \). Then:

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

\[
\Delta_c \overset{\text{def}}{=} \sum_{k \gg 1} \Delta_c(l - k, \epsilon_k) \in \mathbb{Z}_2^{F-1},
\]

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

(c) In the exceptional case, we have \( \Delta_c \in \mathbb{Z}_2^F \) provided that either \( c \in \text{Gal}(K^G/L) \) or \( \delta(\epsilon_k) = 0 \).

[Note that in the exceptional case the function \( \delta \) is \( \mathbb{Z}_2 \)-valued because the conductor \( f = (l) \) 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 \( \delta(\epsilon_k) = 1 \) and that \( c \notin \text{Gal}(K^G/L) \). Then \( \Delta_c \) is exactly divisible by \( 2^{F-1} \).

In connection with these theorems, we now explain why the case where each \( \epsilon_k \) has parity \((-1)^k\) is a central one. As in §1, let \( H \) be the subgroup of \( G \) generated by the real Frobenius elements \( \sigma_Y \). Let \( \mathbb{N} : H \to \{2\} \) be the homomorphism such that \( \mathbb{N} \sigma_Y = -1 \) for each \( Y \); it is the restriction to \( H \) of the \( p \)-adic norm character \( \mathbb{N} : G \to \mathbb{Z}_p \) for any prime \( p \).

Suppose that \( \epsilon \) is a function on \( G_x \) with values in a \( \mathbb{Q} \)-vector space. Write

\[
\epsilon^+ = \frac{1}{H} \sum_{c \in H} \epsilon_c,
\]

\[
\epsilon^- = \frac{1}{H} \sum_{c \in H} \mathbb{N} c \cdot \epsilon_c;
\]

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

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

(1) For \( k \gg 1 \) and \( c \in H \) we have

\[ L(1 - k, \epsilon_c) = \mathbb{N} c^k L(1 - k, \epsilon_c). \]
(2) We have

\[ L(l-k, \epsilon) = \begin{cases} 
L(l-k, \epsilon^+) & \text{if } k \text{ is even} \\
L(l-k, \epsilon^-) & \text{if } k \text{ is odd.}
\end{cases} \]

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

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 \( \Lambda_c(0, \epsilon) \) for arbitrary functions \( \epsilon: \mathbb{Z}_p \to \mathbb{Z}_2 \).

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 \( G_p = \varprojlim G \).

4.1. The group previously denoted by \( G \) will now be referred to without abbreviation as \( \text{Gal}(K^{ab}/K) \). We shall reformulate in terms of measures on \( G \) all Kummer congruences modulo the conductors \( f_p^n \) \((n \geq 0)\).

For each locally constant function \( \epsilon: g \to \mathbb{Q} \), quantities \( L(1-k, \epsilon) \in \mathbb{Q} \) are defined for \( k \gg 1 \). Namely, any such \( \epsilon \) is (for sufficiently large \( n \)) a map \( \mathbb{F}_p^n \to \mathbb{Q} \), and the numbers \( L(1-k, \epsilon_n) \) attached to this map as in \( \text{Gal} \) are independent of the choice of \( n \) because of (1.4). For fixed \( k \), the association \( \epsilon \mapsto L(1-k, \epsilon) \) is thus a distribution on \( G \) with values in \( \mathbb{Q} \).

For each locally constant \( \epsilon: g \to \mathbb{Q}_p \) and each \( c \in \text{Gal}(K^{ab}/K) \), we define

\[ \Lambda_c(1-k, \epsilon) = L(1-k, \epsilon) - NC_k L(1-k, \epsilon_0) \in \mathbb{Q}_p \]
as in §2. Since \( N : \text{Gal}(\mathbb{K}_{ab}/\mathbb{K}) \to \mathbb{Z}_{p}^\times \) may be viewed as a function on \( G \), for given \( \epsilon \) and \( k \), a quantity \( \Delta_c(l - k, \epsilon) \) is well defined for \( c \) in \( G \).

For later use, we recall the standard factorization \( N = \langle \rho \rangle \) of the norm character on \( G \) as the product of a character \( x \mapsto \langle x \rangle \) with values in \( 1 + \mathbb{Z}_{p}^\times \) and a \( \mathbb{Z}_{p}^\times \)-valued character of finite order \( \rho \), the Teichmüller character. We let \( \Gamma \subseteq \mathbb{Z}_{p}^\times \) be the image of \( \langle \rho \rangle \); it is (non-canonically) isomorphic to \( \mathbb{Z}_{p} \).

The extension of \( K \) cut out by the character \( \langle \rho \rangle \) is the cyclotomic \( \mathbb{Z}_{p} \)-extension of \( K \).

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

(4.1) \text{THEOREM.} For each \( c \in G \), the distribution \( \epsilon \mapsto \Delta_c(0, \epsilon) \) is a measure \( \mu_c \) on \( G \) with values in \( \mathbb{Z}_{p} \). For \( k \gg 1 \), the measure \( y^{k-1} \mu_c \) is the map \( \epsilon \mapsto \Delta_c(l - k, \epsilon) \).

\text{Proof.} The first statement asserts that if a locally constant function \( c \) on \( G \) is \( \mathbb{Z}_{p} \)-valued, then \( \Delta_c(0, \epsilon) \) 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 \( k \gg 1 \) and \( n \gg 1 \) that

\[ \int \epsilon y^{k-1} d\mu_c \equiv \Delta_c(l - k, \epsilon) \mod p^n \mathbb{Z}_{p} \]

for each locally constant \( \epsilon \colon G \to \mathbb{Z}_{p} \). For this, let \( \eta : G \to \mathbb{Z}_{p} \) be a locally constant function such that \( \eta \equiv y^{k-1} \mod p^n \). By congruence \( B \) of §2, we have

\[ \Delta_c(l - k, \epsilon) \equiv \Delta_c(0, \epsilon \eta) \mod p^n \mathbb{Z}_{p} \].

On the other hand, because \( \mu_c \) is a measure, we have

\[ \Delta_c(0, \epsilon \eta) = \int \epsilon \eta d\mu_c \equiv \int \epsilon y^{k-1} d\mu_c \mod p^n \mathbb{Z}_{p} \].

This completes the proof.

\text{Remark.} Conversely, we recover the Kummer congruences \( \mod p^n \) \((n \gg 0)\) from the measures \( \mu_c \) as follows: if \( \int \epsilon y^{k-1} d\mu_c \) is \( \mathbb{Z}_{p} \)-valued, then we have

\[ \Delta_c(l - k, \epsilon) \equiv \int \epsilon y^{k-1} d\mu_c \in \mathbb{Z}_{p} \].

187
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 \( \lambda_c \equiv N^{-1} \psi_c \). Then \( \lambda_c \) is a measure on \( G \) with the property that

\[
\int \epsilon \pi^{k} \, d\lambda_c = \lambda_c(1 - k, \epsilon)
\]

for \( k \geq 1 \) and \( \epsilon \) locally constant (cf. [6, 3.5]).

In the language of [6], the measures \( \lambda_c \) define a pseudo-measure \( \lambda \) on \( G \). For each non-trivial continuous character \( \psi \) on \( G \) with values in the completion \( \mathbb{Q}_p \) of the algebraic closure of \( \mathbb{Q}_p \), an integral

\[
\int \psi \, d\lambda = \int \frac{\psi \pi^{k}}{1 - \psi(c)} \, d\lambda_c \quad (c \in \mathbb{Q}_p)
\]

is defined independently of \( c \). When \( \psi \) is a character of finite order, we have in particular

\[
\int \psi \pi^{k} \, d\lambda = \lambda(1 - k, \psi).
\]

(4.3) Suppose that Leopoldt's conjecture is true for \( K \) and \( p \), i.e., that the group \( A = \text{Ker}(\lambda) \) is finite. Then by [6, 1.15], \( \lambda \) may be uniquely written as the sum of a \( \mathbb{Z}_p \)-valued measure \( \mu \) on \( G \) and some \( \mathbb{Z}_p \)-multiple of a certain "standard" pseudo-measure on \( G \) obtained 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 \( \lambda \) is already a measure. Write \( \mu = \lambda \) in this case. Then in both cases we have at least

\[
\int \psi \, d\lambda = \int \psi \, d\mu \quad \text{for all characters } \psi \text{ which are non-trivial on } A \quad [6, 1.17].
\]

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 \( \text{Gal}(K^{ab}/K) \)).

(4.4) **THEOREM.** Let \( \psi: G \to \mathbb{Z}_p \) be a continuous function which is even in the sense that it is invariant under \( H \). Then for all \( c \in G \) we have

\[
\int \psi \, d\lambda_c \in \mathbb{Z}_p.
\]
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 \( \int \phi \ d\lambda_\xi \) is divisible in \( \mathbb{Z}_p \) by the order of \( \mu \) when \( \phi \) is even. This order divides \( 2^F \), and it is equal to \( 2^F \) 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 \( \mu \) be the measure on \( G \) introduced in (4.3). For all even \( \phi: G \to \mathbb{Z}_p \), we have \( \int \phi \ d\mu \in 2^F \mathbb{Z}_p \).

Proof. The divisibility (4.4) asserts that the pseudo-measure on \( G/\mu \) obtained from \( \lambda \) and the projection \( G \to G/\mu \) is divisible by \( 2^F \). 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 \( \varepsilon \) of finite order on \( G \). Let \( E \) be the finite extension of \( \mathbb{Q}_p \) generated by the values of \( \varepsilon \), and let \( R \) be the integer ring of \( E \). By definition \( L_p(s, \varepsilon) \) is the continuous function (of \( s \)) on \( \mathbb{Z}_p - \{0\} \) 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

\[
(4.6) \quad \frac{1}{1 - \varepsilon(c)(c)^{1-s}} \int x^{s} \varepsilon(x) d\lambda_\xi(x)
\]

then represents a continuous function of \( s \) having the defining property of \( L_p(s, \varepsilon) \). Alternately, \( L_p(s, \varepsilon) \) is simply the integral of \( \varepsilon(c)^{1-s} \) against the pseudo-measure \( \lambda \).

The analyticity properties result from 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 $\Gamma \times \Lambda$. Also, let $\gamma \in \Gamma$ be a topological generator of $\Gamma$ over $\mathbb{Z}_p$. If $\alpha : \Gamma \to \mathbb{Z}_p^*$ is the resulting isomorphism, we have $x = \gamma^{\alpha(x)}$ for $x \in \Gamma$. We write simply $\alpha$ for the composite of $\alpha$ with the projection $G \to \Gamma$.

Let $\psi$ be a continuous character on $G$ with values in $\mathbb{C}^*$. It is the product of a character $\psi_A$ on $G$ which is trivial on $\Gamma$ and the character $x \mapsto u^{\alpha(x)}$, where $u = \psi(\gamma)$. For $n \geq 0$, let $a_n$ be the integral
\[
\int_{\Gamma} \psi_A(x) \left( \frac{u(x)}{n} \right)^n du(x) \in \mathbb{R},
\]
where $\left( \frac{u(x)}{n} \right)^n$ is the $n^{th}$ binomial function on $\mathbb{Z}_p^*$, viewed via $\alpha$ as a function on $\Gamma$. Then, by the binomial theorem, we have
\[
(4.7) \quad \int_{\Gamma} \psi_A = \sum_{n \geq 0} \frac{a_n (u - 1)^n}{n!},
\]
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 $\psi : \mathbb{Z}_p \to \mathbb{R}$ is Iwasawa analytic if there is a power series $F \in \mathbb{R}[[T]]$ such that $F(\tau^{l-1} - 1) = \psi(\tau)$. [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 $\gamma$ of $\Gamma$.] Here are the main facts concerning $L_p(s, \varepsilon)$:

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

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

**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 \( \psi = ( \cdot)^{1-\delta} \) and \( \mu = \varepsilon \zeta \). The divisibility of the coefficients of the power series representing the numerator is a consequence of (4.4) and the hypothesis that \( \varepsilon \) is an even character. (It is worth noting, in passing, that when \( \varepsilon \) 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 \( \mathbb{H}([T]) \) (cf. [4], 6.5). A more direct approach is to use the expression

\[
L_p(s, \varepsilon) = \int \varepsilon(\cdot)^{1-\delta} d\mu,
\]

valid when \( \varepsilon \) is non-trivial on \( A \), for \( L_p(s, \varepsilon) \) in terms of the measure \( \mu \) of (4.3). The divisibility of \( F_\varepsilon \) by \( z^T \) results from (4.5).

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

\[
L_p(s, \varepsilon \delta) = \int (\cdot)^{1-\delta \varepsilon} d\lambda
\]

\[
= F_\varepsilon(\gamma^{1-\delta \varepsilon}(\gamma) - 1).
\]

**BIBLIOGRAPHY**


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