Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 9, 8 p.

14 novembre 1977

p-ADIC L-FUNCTIONS ATTACHED TO CHARACTERS OF p-POWER ORDER

par Kenneth A. RIBET

SOMMAIRE. - L'objet de ce papier (rédigé en anglais) est d'étudier la fonction L p-adique (p impair) attachée à un caractère ε d'ordre une puissance de p dont le conducteur n'est pas une puissance de p . On donne un critère pour la non-trivialité de cette fonction. On trouve aussi que, si l'on remplace ε par le produit de ε et une puissance paire et non triviale du caractère de Teichmüller mod p , la fonction L qu'on obtient est toujours non triviale.

1. As is well known, the values at negative integers of the L-series attached to a function $\varepsilon : \mathbb{Z}/f\mathbb{Z} \longrightarrow \mathbb{C}$ are given by universal formulas as rational linear combinations of the values of ε . This fact permits us to define, when ε is a periodic function on $\mathbb{Z}$ with values in a $\mathbb{Q}$-vector space V , elements $L(1-k , \varepsilon) \in V$, for $k \geqslant 1$. One is especially interested in the case where V is a number field or, after completion, a p-adic field .

If ε is a character $(\mathbb{Z}/f\mathbb{Z})^* \longrightarrow \overline{\mathbb{Q}}_p^*$ (extended by 0 to a function on $\mathbb{Z}/f\mathbb{Z}$), there are well known necessary and sufficient conditions for the integrality of a number $L(1-k , \varepsilon) \in \overline{\mathbb{Q}}_p$ ([C], [F], [Le]). In this paper, we shall recall a proof of the sufficiency of the conditions in the case $p \neq 2$. At the same time, we find a criterion for the valuation of certain numbers $L(1-k , \varepsilon)$ to be strictly positive.

Our tools are the "Kummer congruences" as given by MAZUR [M] (and [K], [L]), and the (consequent) theory of p-adic L-functions. These can be used to prove as well some "trivial divisibilities" of L-values for $p = 2$ (cf. [Gr]), and also, of course, the necessity of the conditions for integrality, not merely their sufficiency. Our motivation in recalling the deduction of integrality theorems for the $L(1-k , \varepsilon)$ from the Kummer congruences was that these L-values occur as the constant terms in the q-expansions of certain Eisenstein series $G_{k,\varepsilon}$ for congruence subgroups of $SL_2 \mathbb{Z}$. One can ask if more generally modular forms of the same "type" as a $G_{k,\varepsilon}$ will have constant terms enjoying the same integrality properties as the corresponding $L(1-k , \varepsilon)$ if their non-constant terms are integral. An example given in the last paragraph shows that this is not the case.

2. Given a periodic function $\varepsilon : \mathbb{Z} \longrightarrow V$ as in § 1 and an element $c \in \hat{\mathbb{Z}}^*$, we let ε_c be the function $x \longmapsto \varepsilon(cx)$. For $k \geqslant 1$, we set

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

where c_p is the image of c under the projection $\hat{\mathbb{Z}}^* \longrightarrow \mathbb{Z}_p^*$.

The Kummer congruences that we need may be stated as follows. Let $\varepsilon_1 , \ldots , \varepsilon_t$

be periodic functions on $\mathbb{Z}$ with values in $\mathbb{Q}_p$, and let $k_1, \ldots, k_t \geq 1$. Suppose that, for $n \geq 1$; we have

$$\sum_{i=1}^{t} \varepsilon_i(n)n^{k_i-1} \in \mathbb{Z}_p .$$

Then we have

$$\sum_{i=1}^{t} \Delta_c(1-k_i , \varepsilon_i) \in \mathbb{Z}_p .$$

Equivalently, we may regard periodic functions on $\mathbb{Z}$ as the <u>locally constant</u> functions on $\hat{\mathbb{Z}}$. The Kummer congruences state that the map $\varepsilon \longmapsto \Delta_c(0, \varepsilon)$ is a measure μ_c on $\hat{\mathbb{Z}}$ with values in $\mathbb{Z}_p$ such that

$$\int \varepsilon(x)x_p^{k-1}\, d\mu(x) = \Delta_c(1-k , \varepsilon) ,$$

for all $k \geq 1$, and all locally constant ε. (Here again, x_p is the projection function $\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}_p$.)

Suppose that ε is a character of conductor $f \geq 1$ with values in $\bar{\mathbb{Q}}_p^*$, where p is an odd prime. Let K be the finite extension of $\mathbb{Q}_p$ generated by the values of ε, and let R be the integer ring of K. When is a value $L(1-k , \varepsilon)$ an element of R (i. e., integral)? Using the fact that the values of ε lie in R (which is a free $\mathbb{Z}_p$-module), we find by the Kummer congruences the integrality

$$\Delta_c(1-k , \varepsilon) = (1-\varepsilon(c)c_p^k).L(1-k , \varepsilon) \in R$$

for each $c \in \hat{\mathbb{Z}}^*$. This implies that $L(1-k , \varepsilon)$ is itself integral, <u>except</u> perhaps in the special case where the product of ε and the k-th power of the Teichmüller character is a character of p-power order. (Recall that the Teichmüller character is the unique character $\omega : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \mathbb{Z}_p^*$ which satisfies $\varepsilon(x) \equiv x \mod p$, for all $x \in (\mathbb{Z}/p\mathbb{Z})^*$.)

Said differently, if the order of ε is divisible by a prime other than p, we have

$$L(1-k , \varepsilon\omega^{-k}) \in R$$

for $k \geq 1$. On the other hand, suppose that the order of ε is a power of p; this implies, incidentally, that ε is an even character since p is odd. One then finds in the literature, the additional statement that a number $L(1-k, \varepsilon\omega^{-k})$ lies in R if (and only if) the conductor of ε is divisible by some prime different from p.

3. The theory of p-adic L-functions provides a proof of the integrality. Indeed, let ε, once again, be a character of p-power order whose conductor f is not a p-power. Since ε is non-trivial, there is a continuous function $L_p(s , \varepsilon)$ on $\mathbb{Z}_p$ whose value at $1-k$ is

$$L^*(1-k , \varepsilon\omega^{-k}) = L(1-k , \varepsilon\omega^{-k})(1-p^{k-1}(\varepsilon\omega^{-k})(p)) .$$

The factor multiplying $L(1-k , \varepsilon^{-k})$ is trivial unless $p-1|k$; hence it is in all cases a unit. Thus the integrality of $L^*(1-k , \varepsilon\omega^{-k})$ is equivalent to that of $L(1-k, \varepsilon\omega^{-k})$.

Let $\langle x\rangle$ be the function $x \longmapsto x\omega(x)^{-1}$ on $\mathbb{Z}_p^*$. We view it alternately as a function on $\hat{\mathbb{Z}}^*$ via the projection $x \longmapsto x_p$. As we shall recall in § 5 , there is, for each $c \in \hat{\mathbb{Z}}^*$, a power series $F_c(T) \in R[[T]]$ such that

$$F_c((1+p)^{-s}-1) = (1-\varepsilon(c)\langle c\rangle^{1-s})L_p(s, \varepsilon)$$

for all $s \in \mathbb{Z}_p$. (The appearance of the quantity $1+p$ in this representation arises from the choice of an isomorphism of $\mathbb{Z}_p$-modules

$$\alpha : 1 + p\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_p$$

such that $x = (1+p)^{\alpha(x)}$ for all x in the multipli ative group $1+p\mathbb{Z}_p$. For simplicity, we write again $\alpha(x)$ for the function $\alpha(\langle x\rangle)$ on $\mathbb{Z}_p^*$ (or $\hat{\mathbb{Z}}^*$).) Since we have on the other hand

$$1-\varepsilon(c)\langle c\rangle^{1-s} = 1-\varepsilon(c)\langle c\rangle(1+T)^{\alpha(c)}|_{T=(1+p)^{-s}-1} ,$$

we can "represent" $L_p(s, \varepsilon)$ by a quotient of two power series with coefficients in R . Now the point is that, although the individual series representing the "fudge factors" $1-\varepsilon(c)\langle c\rangle^{1-s}$ are not invertible in $R[[T]]$, it is easy to see that their greatest common divisor in $R[[T]]$ is 1 ([CL], p. 540). Hence there is an $F \in R[[T]]$ such that

$$F((1+p)^{-s}-1) = L_p(s, \varepsilon) .$$

In particular, the values $L_p(1-k, \varepsilon)$ belong to R , which is what we wanted to show.

4. A different proof of the integrality may be given using the measures μ_c of § 2. We view $\varepsilon\omega^{-k}$ and ω^{-k} as characters of $(\mathbb{Z}/fp\mathbb{Z})^*$. These give rise to two functions on $\mathbb{Z}/fp\mathbb{Z}$, whose values are zero on the non-invertible elements. We regard them as functions φ_1 and φ_2 on $\hat{\mathbb{Z}}$, which are constant mod pf . If $\mathfrak{P}$ is the maximal ideal of R , we have

$$\varphi_1(x) \equiv \varphi_2(x) \mod \mathfrak{P}$$

for all $x \in \hat{\mathbb{Z}}$. Multiplying this congruence by x_p^{k-1} and integrating, we find the Kummer congruence

$$\Delta_c(1-k, \varphi_1) \equiv \Delta_c(1-k, \varphi_2) \mod \mathfrak{P} .$$

The first of these two numbers is simply $(1-\varepsilon(c)\langle c\rangle^k)L^*(1-k, \varepsilon\omega^{-k})$. The second is

$$(1-\langle c\rangle^k)L^*(1-k, \omega^{-k}) \prod_{\ell | f, \ell \neq p}(1-\omega^{-k}(\ell)\ell^{k-1})$$

(the factors ℓ are understood to be primes) because in φ_2 we have artificially given ω^{-k} the value 0 on <u>all</u> primes dividing pf . Now it is clear that any $\ell \neq p$ which divides f is congruent to 1 mod p , and so in the product (which by hypothesis is non empty) every term is divisible by p . Since on the other hand the term multiplying the product is integral (again by a Kummer congruence, for example), the right hand side of the above Kummer congruence is divisible by $\mathfrak{P}$. Looking now at the left side of the congruence, we choose a c such that $\varepsilon(c)$ generates the group of values of ε. We then have $\mathfrak{P} \| (1 - \varepsilon(c)\langle c\rangle^k)\|$, implying the integrality of $L^*(1-k, \varepsilon\omega^{-k})$. We note that our congruence now reads $0 \equiv 0$; we cannot obtain from it the value of $L^*(1-k, \varepsilon\omega^{-k}) \bmod \mathfrak{P}$.

As a variant, let us replace ε by $\varepsilon\omega^i$, where $i \not\equiv 0 \pmod{p-1}$ is even. We obtain as above the congruence

$$(1 - \varepsilon(c)\omega^i(c)\langle c\rangle^k)L^*(1-k, \varepsilon\omega^{i-k}) \equiv 0 \mod \mathfrak{P} .$$

Since ω^i is non trivial, we may choose c so that the "fudge factor" is invertible mod $\mathfrak{P}$. This implies the ("trivial") divisibility by $\mathfrak{P}$ of the L^*-value. The passage from L to L^* just means multiplying by an Euler factor at p; as before we see that this factor is trivial for $k = 1$, and hence a unit for all k. The conclusion is that we have

$$\mathfrak{P} | L(1-k, \varepsilon\omega^{i-k})|$$

for all $k \geqslant 1$.

5. We obtain a congruence mod $\mathfrak{P}$ for the numbers $L(1-k, \varepsilon\omega^{-k})$ by combining the techniques of § 3 and § 4. The point is that we have a (term by term) congruence of <u>series</u> $F_c \equiv G_c \mod \mathfrak{P}$, where F_c is the series of § 3 representing

$$A(s) = (1 - \varepsilon(c)\langle c\rangle^{1-s})L_p(s, \varepsilon) ,$$

and G_c represents similarly the regularized p-adic zeta function

$$B(s) = [(1 - \langle c\rangle^{1-s})\zeta_p(s)] \prod_{\ell | f, \ell \neq p}(1 - \ell^{-s})$$

which has been stripped of its ℓ-Euler factors for primes $\ell | f$. (The idea of looking at such congruences of series was suggested by Lichtenbaum.) The congruence is easy to prove, once we remember that we can construct the series F_c and G_c by regarding $A(s)$ and $B(s)$ as p-adic Mellin transforms of measures. Indeed, we have

$$A(s) = \int_{\hat{\mathbb{Z}}} \langle x\rangle^{-s} \ \varepsilon(x)\omega^{-1}(x) \ d\mu_c(x) ,$$

with the convention that the integrand is given the value 0 for x such that $x_p \notin \mathbb{Z}_p^*$. (To prove this identity, we note that the integral is continuous in s and, by the defining properties of μ_c, coincides with $A(s)$ for $s = 1-k$, $k \geqslant 1$.) Similarly, we have

$$B(s) = \int \langle x\rangle^{-s} \ \psi(x)\omega^{-1}(x) \ d\mu_c(x) ,$$

where the integral is again taken over the subset S of $\hat{\mathbb{Z}}$ consisting of those x with $x_p \in \mathbb{Z}_p^*$, and where ψ is the characteristic function of $(\mathbb{Z}/fp\mathbb{Z})^*$ in $\mathbb{Z}/fp\mathbb{Z}$. For $x \in S$, the binomial theorem gives

$$\langle x\rangle^{-s} = \sum_{n\geq 0}\binom{\alpha(x)}{n}\gamma_s^n ,$$

where $\gamma_s = (1+p)^{-s} - 1$. Putting this into the integrals, we find

$$A(s) = \sum_{n\geq 0} a_n \gamma_s^n , \quad B(s) = \sum_{n\geq 0} b_n \gamma_s^n ,$$

where

$$a_n = \int \binom{\alpha(x)}{n} \varepsilon(x)\omega^{-1}(x)\, d\mu_c(x) , \quad b_n = \int \binom{\alpha(x)}{n} \psi(x)\omega^{-1}(x)\, d\mu_c(x) ;$$

both integrals are taken over S . Now $\varepsilon \equiv \psi \mod \mathfrak{P}$, and hence $a_n \equiv b_n \mod \mathfrak{P}$ for each n ; this is exactly the congruence required.

Let c be an element of $\hat{Z}^*$ such that $\langle c\rangle = 1 + p$, i. e., such that $\alpha(c) = 1$. The first factor in the expression for $B(s)$, namely $(1 - \langle c\rangle^{1-s})\zeta_p(s)$, may be written in the form $H_c(\gamma_s)$, for some series H_c with coefficients in R . It is easy to see that H_c is invertible, for we have more precisely the congruence

$$H_c(0) = - p\zeta_p(0) = - pL(0 , \omega^{-1}) \equiv + 1 \mod p .$$

The remaining factors in the expression for $B(s)$ are also represented by power series : we have

$$G_c(T) = H_c(T) \prod[1 - (1 + T)^{\alpha(\ell)}] ,$$

with the product as usual taken over the primes ℓ dividing f and different from p . Since $\langle c\rangle = 1 + p$ and $\varepsilon(c) \equiv 1 \mod \mathfrak{P}$, we have

$$F_c(T) = [1 - \langle c\rangle\varepsilon(c)(1 + T)]F(T) \equiv - TF(T) \mod \mathfrak{P} .$$

Hence, we obtain finally

$$- TF(T) \equiv H_c(T) \prod[1 - (1 + T)^{\alpha(\ell)}] \mod \mathfrak{P} .$$

This formula shows that not all coefficients of $F(T)$ are divisible by $\mathfrak{P}$ (we have "$\mu = 0$") and enables one to compute the Weierstrass degree of F .

More precisely, we find that $F(T)$ is the product of an invertible power series with a distinguished polynomial $W(T)$ of degree

$$\lambda = - 1 + \sum_{\ell | f'} \left\{\frac{\ell - 1}{p}\right\}_{p'} ,$$

where $\{n\}_p$ means the p-part of an integer n , and f' is the prime to p part of f . In particular, we have $\lambda > 0 \Longleftrightarrow p^2|\varphi(f')$, where φ is the Euler function. Another way to say that $W(T)$ is of positive degree is to say that $F(0)$ is divisible by $\mathfrak{P}$. It is exactly divisible by $\mathfrak{P}$ if and only if $W(T)$ is an Eisenstein polynomial. (Observe that if $W(T)$ is an Eisenstein polynomial and $\lambda > 1$, then the roots of $W(T)$ do not lie in K . This is rather the opposite of what occurs in the familiar situation of a p-adic L-function attached to a power of ω , where in all examples so far we have $\lambda = 0$ or 1. I have no conjecture concerning the precise values of the roots.) A final remark is that we have the congruence

$$F(0) \equiv L_p(s , \varepsilon) \mod p$$

for all $s \in \mathbb{Z}_p$. A number $L(1-k, \varepsilon\omega^{-k})$ is thus divisible by $\wp$ if and only if $p^2 | \varphi(f')$. For comparison, we recall that the numbers $L(1-k, \varepsilon\omega^{i-k})$ (i even and $i \not\equiv 0 \mod p-1$) are always divisible by $\wp$.

The number $F(0) = L(0, \varepsilon\omega^{-1})$ occurs in the formula for the relative class number of the (imaginary) abelian field corresponding to the kernel of $\varepsilon\omega^{-1}$. Provided that the degree of this field is no bigger than 256, we can decide the power of $\wp$ dividing $F(0)$ by consulting the table [SR]. For $p = 3$ and

$$f = 19 , 37 , 73 , 91 \ (= 7 \times 13) , 109 , 127 , \text{ or } 133 \ (= 7 \times 19) ,$$

we have $\wp \| F(0)$, except in the case where $f = 133$ and ε is of order 9, in which case $\wp^3 | F(0)$. This extra divisibility can be explained by an argument similar to the above, which begins with the observation that ε is congruent mod $\wp^3$ to a character of order 9 mod 19. As far as I can see, it is only an accident that one gets exactly the divisibilities which are a priori predictable. In an analogous series of examples, we take $p = 5$ and look at values $L(0, \varepsilon\omega)$, with ε of order 5 and conductor $f = 11 , 31 , 41 , 61$. Here we find a trivial divisibility $\wp | L(0, \varepsilon\omega)$ and no further divisibility except in the case $f = 31$, when $\wp^2 | L(0, \varepsilon\omega)$. This extra divisibility seems "irregular".

6. As mentioned just above, our trivial divisibilities for L-values give divisibilities for relative class numbers of certain imaginary abelian fields. For example, if $p \geqslant 5$, and N is a product of distinct primes congruent to 1 mod p, the field of pN-th roots of 1 has a relative class number divisible by p.

On hearing of these results, LENSTRA, GREENBERG and GRAS each pointed out that there is a simple algebraic interpretation. In the example of pN-th roots of 1, the ideal classes generated by the (ramified) primes dividing N in $\mathbb{Q}(\mu_{pN})$ are non trivial and highly independent. GRAS suggests that the existence of these ideal classes may be predicted by Chevalley's theory of ambiguous classes in cyclic extensions ([Ch], p. 402-406), which has recently been refined in [G].

7. The connection with modular forms is the following. Let ε be a character mod f with values in $\bar{\mathbb{Q}}_p^*$, and let $g = \sum_{n\geq 0} a_n q^n$ be a modular form of weight k and character $\varepsilon\omega^{-k}$ with coefficients in $\bar{\mathbb{Q}}_p$. Suppose that the a_n, with $n > 0$, are (p-adically) integral. Then for each $c \geqslant 1$ prime to pf one can show that

$$(1 - \varepsilon(c)\omega^{-k}(c)c^k)a_0$$

is integral (cf. [Ka]). As in § 2, it follows from this "Kummer congruences" that a_0 is integral if ε is not of p-power order. If ε has p-power order and p-power conductor, then a_0 will not, in general, be integral ; this is seen from the example of the Eisenstein series

$$G_{k,\eta} = \frac{L(1-k, \eta)}{2} + \sum_{n\geq 1}(\sum_{d|n} \eta(d)d^{k-1})q^n ,$$

where $\eta = \varepsilon\omega^{-k}$.

The remaining case is that where ε has p-power order but not p-power conductor. Then as we have seen, the constant term of $G_{k,\varepsilon}$ is integral, and this integrality can be directly traced to Kummer congruences. This leads one to speculate that, more generally, the term a_0 might always be integral.

Here is an example where this is not true. We take $p = 3$ and $k = 2$, so that in particular we will have $\varepsilon = \varepsilon\omega^{-k}$. Let f be a prime congruent to $1 \bmod 3$ but not mod 9. Let ε be one of the two characters mod f of order 3, with values in $K = \mathbb{Q}_3(\mu_3)$. Let g be the difference between $G_{2,\varepsilon}$ and the ("other") Eisenstein series

$$H_{2,\varepsilon} = \sum_{n\geq 1}(\sum_{d|n} \varepsilon(\tfrac{n}{d})d)q^n$$

of weight 2 and character ε. By the results of § 5, the constant coefficient $L(-1, \varepsilon)/2$ of g is a unit in K since $9 \nmid \varphi(f)$. (This can also be checked directly by using the formula for an $L(-1)$.) On the other hand, we shall see that the higher coefficients of the q-expansion of g are divisible by the maximal ideal $\mathfrak{P}$ of the integer ring of K.

To prove this, since both $G_{2,\varepsilon}$ and $H_{2,\varepsilon}$ are eigenforms for the Hecke operators, it is enough to check the congruence

$$1 + \varepsilon(\ell)\ell \equiv \ell + \varepsilon(\ell) \mod \mathfrak{P}$$

for each <u>prime</u> ℓ. This is of course a consequence of the congruence $\varepsilon \equiv 1 \mod \mathfrak{P}$, <u>except</u> when $\ell = f$, in which case $\varepsilon(\ell) = 0$. But in the case $\ell = f$, the congruence to be proved reads $1 \equiv f$; it is true mod $\mathfrak{P}$ because true mod 3.

BIBLIOGRAPHY

[C] CARLITZ (L.). - Arithmetic properties of generalized Bernoulli numbers, J. für reine und angew. Math., t. 202, 1959, p. 174-182.

[Ch] CHEVALLEY (C.). - Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sc. Tokyo, Section 1, t. 2, 1933, p. 365-476.

[CL] COATES (J.) and LICHTENBAUM (S.). - On ℓ-adic zeta functions, Annals of Math., Series 2, t. 98, 1973, p. 498-550.

[F] FRESNEL (J.). - Valeurs des fonctions zêta aux entiers négatifs, Séminaire de théorie des nombres de l'Université de Bordeaux, Année 1970/71, exposé nº 27.

[G] GRAS (G.). - Nombres de φ-classes invariantes ; application aux classes des corps abéliens, Bull. Soc. math. France (to appear).

[Gr] GREENBERG (R.). - On 2-adic L-functions and cyclotomic invariants, Math. Z., t. 159, 1978, p. 37-45.

[Ka] KATZ (N.). - p-adic properties of modular schemes and modular forms. "Modular functions of one variable, III [1972, Antwerpen]", p. 69-190. - Berlin, Springer-Verlag, 1973 (Lecture notes in Mathematics, 350).

[K] KOBLITZ (N.). - p-adic numbers, p-adic analysis, and zeta functions. - Berlin, Springer-Verlag, 1977.

[L] LANG (S.). - Introduction to cyclotomic fields (to appear).

[Le] LEOPOLDT (H.-W.). - Eine Verallgemeinerung der Bernoullischen Zahlen., Abh. Math. Sem. Univ. Hamburg, t. 22, 1958, p. 131-140.

[M] MAZUR (B.). - Unpublished Bourbaki report on p-adic measures, 1972.

[SR] SCHRUTKA v. RECHTENSTAMM (G.). - Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, Abh. Deutsch. Akad. Wiss. Berlin Kl. math. Phys. Techn., t. 2, 1964, 64 p.

(Texte remis le 20 mars 1978)

Kenneth RIBET
Mathématiques, Bâtiment 425
Université de Paris-Sud
91405 ORSAY