A CHARACTERIZATION OF THE $\lambda$-INVARIANT OF A $p$-ADIC $L$-FUNCTION

TAUNO METSÄNKYLÄ

1. Let $p$ be a prime, and put $q=p$ if $p>2$ and $q=4$ if $p=2$. Consider the Kubota—Leopoldt $p$-adic $L$-function $L_p(s, \theta)$ attached to an even non-principal character $\theta$. Write $\theta = \chi \omega$, where $\omega$ is the Teichmüller character mod $q$ and $\chi$ is a character with conductor not divisible by $pq$ (all characters are assumed primitive). It is well known that $L_p(s, \chi \omega)$ has a power series expression, say

$$f(X, \chi \omega) = \sum_{j=0}^{\infty} a_j X^j,$$

whose coefficients $a_j$ are integers of the field $\mathbb{Q}_p(\chi)$ generated by the values of $\chi$ over the field of $p$-adic numbers.

By the Ferrero—Washington theorem [2], there exists an index $j$ such that $a_j$ is prime to $p$. The least such index is called the $\lambda$-invariant of $f(X, \chi \omega)$ and denoted by $\lambda = \lambda_f$. Observe that $\lambda$ is characterized by the statement

$$\lambda \equiv h \iff a_0 \equiv a_1 \equiv \ldots \equiv a_{h-1} \equiv 0 \pmod{p},$$

where $h$ denotes a positive integer and $p$ is the maximal ideal of the integer ring of $\mathbb{Q}_p(\chi)$. Another characterization of the $\lambda$-invariant is given in the present note; see the theorem in Section 2. This has proved useful in some problems concerning $\lambda$.

2. To formulate the theorem, we introduce the necessary notation and record some preliminary facts.

Let us write the conductor of the character $\chi$ in the form

$$f_\chi = d \quad \text{or} \quad dq, \quad (d, p) = 1.$$ 

For $n \geq 0$, denote by $\Gamma_n$ the multiplicative group of those residue classes $a + dq p^n \mathbb{Z}$ for which $a \equiv 1 \pmod{dq}$. Let $\gamma_n(a)$ denote the image of $a + dq p^n \mathbb{Z}$ under the canonical projection $(\mathbb{Z}/dq p^n \mathbb{Z})^\times \to \Gamma_n$. Since $\Gamma_n$ is generated by $\gamma_n(1 + dq)^{-1}$, we see that the set $I_n = \{a \in \mathbb{Z}: 0 < a < dq p^n, (a, dq) = 1\}$ can be partitioned into the subsets

$$I_{nk} = \{a \in I_n: \gamma_n(a) = \gamma_n(1 + dq)^{-k}, \quad k = 0, \ldots, p^n - 1\}.$$ 

The power series $f(X, \chi \omega)$ is defined by the congruences

$$f(X, \chi \omega) \equiv \sum_{k=0}^{p^n-1} c_{nk} (1 + X)^k \pmod{(1 + X)^{p^n} - 1},$$

where the coefficients $c_{nk}$ are integers of $Q_p(\chi)$ having the following expressions:

$$c_{nk} = -\frac{1}{dp^n} \sum_{a \in I_{nk}} a\chi(a)$$

(see [5, § 7.2]; cf. also [3] where the definition of $f(X, \chi\omega)$ differs from the present one by a factor $1/2$). Note that the coefficients of $f(X, \chi\omega)$ can be given explicitly as follows:

$$a_j \equiv \sum_{k=j}^{p^n-1} {k \choose j} c_{nk} \pmod{p}, \quad j = 0, \ldots, p^n - 1.$$

Now let $b$ be a positive integer prime to $dp$. For $n \geq 0$ and $k, j = 0, \ldots, p^n - 1$, set

$$S_{nk} = -\sum_{a \in I_{nk}} \chi(a) \left[ \frac{ba}{dp^n} \right], \quad T_j^{(n)} = \sum_{k=j}^{p^n-1} {k \choose j} S_{nk},$$

where $[z]$ denotes the largest integer $\leq z$.

**Theorem.** Let $n \geq 0$ and $1 \leq h \leq p^n$.

(i) If $\lambda \equiv h$, then $T_0^{(0)} = T_1^{(0)} = \ldots = T_{h-1}^{(0)} \equiv 0 \pmod{p}$.

(ii) If $T_0^{(0)} = T_1^{(0)} = \ldots = T_{h-1}^{(0)} \equiv 0$ and $\chi(b)b \equiv 1 \pmod{p}$, then $\lambda \equiv h$.

Note that the expression of $T_j^{(n)}$ is integral, contrary to that of $a_j$. This makes the theorem suitable for the computation of $\lambda$. In fact, Ernvall has carried out such computations by using a similar result which may be regarded as a preliminary version of the above theorem (see [1]). We point out that in that version, proved for $p > 2$ only, the definition of $T_j^{(n)}$ is slightly different and the restriction imposed on $h$ is stronger (the present assumption about $h$ being the natural one). The following proof is completely different; its key idea goes back to the author's article [4] concerning the estimation of $\lambda$ from above. This shows, conversely, that the present theorem also plays an important role in this estimation result.

3. For the proof of the theorem, we keep $n \geq 0$ fixed. We extend the preceding definition of $I_{nk}$ for all $k \in \mathbb{Z}$ by taking $I_{nk} = I_{nm}$ whenever $k \equiv m \pmod{p^n}$. Choose $t \in \mathbb{Z}$ such that

$$\gamma_n(b) = \gamma_n(1+dp)^{-t}, \quad 0 \leq t \leq p^n - 1.$$

The crucial formula of the proof reads

$$S_{nk} = bc_{nk} - \chi(b)^{-1}c_{n,k+t}, \quad k = 0, \ldots, p^n - 1;$$

(3)

this will be verified by an argument similar to [4, Lemma 1]. Indeed, let $a$ run through $I_{nk}$ and write

$$ba = dp^n \left[ \frac{ba}{dp^n} \right] + r_a.$$

Since

$$\gamma_n(r_a) = \gamma_n(ba) = \gamma_n(1+dp)^{-k-t},$$

$$\gamma_n(b) = \gamma_n(1+dp)^{-t}, \quad 0 \leq t \leq p^n - 1.$$
we find that \( r_a \) runs through \( I_{n,k+t} \). Hence we may write
\[
\chi_{n,k+t} = -\frac{1}{dq\cdot p^n} \sum_{a \in I_{nk}} r_a \chi(r_a),
\]
and the right-hand side of (3) becomes
\[
-\frac{1}{dq\cdot p^n} \sum_{a \in I_{nk}} (ba \chi(a) - r_a \chi(b)^{-1} \chi(r_a)) = -\frac{1}{dq\cdot p^n} \sum_{a \in I_{nk}} (ba - r_a) \chi(a).
\]
This proves the claim.

It follows from (3) that
\[
T_j^{(n)} = b \sum_{k=j}^{p^n-1} \left( \begin{array}{c} k \\ j \end{array} \right) c_{nk} - \chi(b)^{-1} \sum_{k=j}^{p^n-1} \left( \begin{array}{c} k \\ j \end{array} \right) \chi_{n,k+t} \quad (j = 0, \ldots, p^n - 1).
\]
By (2), the first sum on the right-hand side is congruent to \( a_j \) (mod p). As for the second sum, we show that
\[
\sum_{k=j}^{p^n-1} \left( \begin{array}{c} k \\ j \end{array} \right) \chi_{n,k+t} \equiv a_j - \sum_{i=0}^{j-1} d_i a_i \quad (\text{mod } p)
\]
\((j=0, \ldots, p^n-1)\), where the coefficients \( d_i \) are rational integers.

We use induction on \( j \). First observe that, as a function of \( k \), \( c_{nk} \) is periodic with period \( p^n \). For \( j=0 \) the left-hand side of (5) equals
\[
\sum_{k=0}^{p^n-1} c_{nk+t} = \sum_{k=0}^{p^n-1} c_{nk} \equiv d_0 \quad (\text{mod } p).
\]
Let \( j \geq 1 \). As usual, set \( \left( \begin{array}{c} k \\ j \end{array} \right) = 0 \) if \( 0 \leq k < j \). Making use of the identity
\[
\left( \begin{array}{c} k+t \\ j \end{array} \right) = \sum_{u=0}^{j} \left( \begin{array}{c} k \\ u \end{array} \right) \left( \begin{array}{c} t \\ j-u \end{array} \right) = \left( \begin{array}{c} k \\ j \end{array} \right) + \sum_{u=0}^{j-1} \left( \begin{array}{c} k \\ u \end{array} \right) \left( \begin{array}{c} t \\ j-u \end{array} \right),
\]
valid for all non-negative \( k \) and \( t \), we obtain
\[
\sum_{k=0}^{p^n-1} \left( \begin{array}{c} k \\ j \end{array} \right) \chi_{n,k+t} = \sum_{k=0}^{p^n-1} \left( \begin{array}{c} k+t \\ j \end{array} \right) c_{n,k+t} - \sum_{u=0}^{j-1} \left( \begin{array}{c} t \\ j-u \end{array} \right) \sum_{k=0}^{p^n-1} \left( \begin{array}{c} k \\ u \end{array} \right) c_{n,k+t}.
\]
Like \( c_{nk} \), also the binomial coefficient \( \left( \begin{array}{c} k \\ j \end{array} \right) \) modulo \( p \) is periodic with period \( p^n \) (apply the above identity and note that \( j \) and \( n \) are positive). Therefore, by the induction hypothesis,
\[
\sum_{k=0}^{p^n-1} \left( \begin{array}{c} k \\ j \end{array} \right) \chi_{n,k+t} \equiv a_j - \sum_{u=0}^{j-1} \left( \begin{array}{c} t \\ j-u \end{array} \right) (d_u - \sum_{i=0}^{u-1} d_i a_i) \quad (\text{mod } p)
\]
with \( d_u \in \mathbb{Z} \). This gives us (5).

From (4) and (5) we conclude that
\[
T_j^{(n)} \equiv (b - \chi(b)^{-1}) a_j + \chi(b)^{-1} \sum_{i=0}^{j-1} d_i a_i \quad (\text{mod } p)
\]
\((j=0, \ldots, p^n-1)\). By comparing this with (1) we easily infer the theorem.
References


University of Turku
Department of Mathematics
SF-20500 Turku
Finland

Received 27 May 1987