Functiones et Approximatio
XXXIX.2 (2008), 223–235

BERNOULLI NUMBERS AND ZEROS OF p-ADIC L-FUNCTIONS

Tauno Metsänkylä

Dedicated to Władysław Narkiewicz
for his 70th birthday

Abstract: Rational p-adic zeros of the Leopoldt–Kubota p-adic L-functions give rise to certain sequences of generalized Bernoulli numbers tending p-adically to zero, and conversely. This relationship takes different forms depending on whether the corresponding Iwasawa λ-invariant is one or greater than one. To understand the relationship better it is useful to consider approximate zeros of those functions.

Keywords: Bernoulli numbers, generalized Bernoulli numbers, p-adic L-functions and their zeros, Iwasawa λ-invariants

1. Introduction

For a prime p and for a nonprincipal even Dirichlet character χ whose conductor is not divisible by p^2 (or by 8, if $p = 2$), consider the Leopoldt–Kubota p-adic L-function $L_p(s, \chi)$. Let θ denote the p-free component of χ. The aim of the present article is to study a relationship between rational p-adic zeros of $L_p(s, \chi)$ and the p-divisibility of the Bernoulli numbers $B^m(\theta)$ as m tends to infinity. As is to be expected, this relationship depends on the Iwasawa λ-invariant attached to χ.

Let ω denote the cyclotomic character mod p when $p > 2$, or the unique character with conductor 4 when $p = 2$. The relationship in question is a direct consequence of the basic formula

$$L_p(1 - m,\, \chi) = -(1 - \chi\omega^{-m}(p)p^{m-1})\frac{B^m(\chi\omega^{-m})}{m} \qquad (m = 1, 2, \ldots). \tag{1.1}$$

It was studied in the recent work [4] by Kellner in the case of ordinary Bernoulli numbers B^m. The present discussion not only contains an extension to $B^m(\theta)$, including $p = 2$, but also treats some new aspects and offers proofs different from [4] that are perhaps more natural and give deeper insight into the results.

2000 Mathematics Subject Classification: primary 11B68, 11R23, 11S40.

2. Preliminaries

Fix an embedding of the field of algebraic numbers into $\mathbb{C}_p$, the completion of an algebraic closure of the p-adic field $\mathbb{Q}_p$. Let v_p denote the p-adic exponential valuation on $\mathbb{C}_p$, normalized so that $v_p(p) = 1$. A congruence $\alpha \equiv \beta (\mathrm{mod}\ p^z)$ in $\mathbb{C}_p$ means that $v_p(\alpha - \beta) \geq z$.

Let α be a rational p-adic integer, that is, $\alpha \in \mathbb{Z}_p$. We define $r_n(\alpha) \in \mathbb{Z}$ by

$$r_n(\alpha) \equiv \alpha \pmod{p^n}, \qquad 0 \leq r_n(\alpha) < p^n .$$

To avoid complications occurring for the prime $p = 2$ we assume throughout sections 2–5 that $p > 2$. The case $p = 2$ is treated in the final section 6.

With the assumptions on χ mentioned above we fix the notation

$$\chi = \theta\omega^t, \qquad 2 \leq t \leq p ,$$

and denote by d the conductor (prime to p) of θ. The reader mainly interested in the case $\theta = 1$ should keep in mind that t then assumes the values $2, 4, \ldots, p-3$.

We introduce the usual difference operator $\Delta_c x_n = x_{n+c} - x_n$ and recall the identity

$$\Delta_{cd} = (1 + \Delta_c)^d - 1. \tag{2.1}$$

The Kummer congruences for $B^m(\theta)$ state, for c divisible by $\varphi(p^h) = (p-1)p^{h-1}$, that

$$\Delta_c^k (1 - \theta(p)p^{m-1}) \frac{B^m(\theta)}{m} \equiv 0 \pmod{p^{hk}} \tag{2.2}$$

whenever $k \geq 0$, $h \geq 1$, $m \geq 1$, with the additional condition $m \not\equiv 0 (\mathrm{mod}\ p-1)$ for $\theta = 1$. These congruences, first proved by Carlitz [2], are in fact crucial for the analyticity of p-adic L-functions. Proofs based on the theory of these functions were presented in [6] and [7].

Recall that $L_p(s, \chi)$ is defined and analytic for all $s \in \mathbb{C}_p$ satisfying $v_p(s) > -1 + \frac{1}{p-1}$. Moreover,

$$L_p(s, \chi) = f_\chi((1 + dp)^s - 1), \tag{2.3}$$

where

$$f_\chi(T) = \sum_{i=0}^{\infty} a_i(\chi) T^i \in \mathcal{O}_\theta[[T]]$$

is the Iwasawa power series. Here $\mathcal{O}_\theta$ is the valuation ring of the field $\mathbb{Q}_p(\theta)$ generated by the values of θ.

By the λ-invariant attached to χ we mean

$$\lambda_\chi = \min\{\, i \geq 0 \mid v_p(a_i(\chi)) = 0 \,\} ,$$

that is, the λ-invariant of the power series f_χ. This power series defines an analytic function on the disc $D_T = \{T \in \mathbb{C}_p \mid v_p(T) > 0\}$, and it follows from the p-adic

Weierstrass Preparation Theorem ([9], Theorem 7.3) that f_χ has λ_χ zeros (counting multiplicities) in D_T. Indeed, these zeros are exactly the zeros of a "distinguished" polynomial of degree λ_χ belonging to $\mathcal{O}_\theta[T]$.

It is easy to see (e.g., [3]) that the zeros T_0 of $f_\chi(T)$ satisfying $v_p(T_0) > \frac{1}{p-1}$ correspond bijectively to the zeros s_0 of $L_p(s,\chi)$; this correspondence is given by

$$T_0 = (1+dp)^{s_0} - 1, \qquad s_0 = \frac{\log(1+T_0)}{\log(1+dp)}. \tag{2.4}$$

In particular, $s_0 = 0$ if and only if $T_0 = 0$, and $v_p(s_0) = v_p(T_0) - 1$ otherwise.

Now consider *rational* p-adic zeros s_0, that is, zeros $s_0 \in \mathbb{Q}_p$. Trivially, $s_0 \in \mathbb{Q}_p$ if and only if $T_0 \in \mathbb{Q}_p$. Since the positive values of v_p in $\mathbb{Q}_p$ are $\geq 1 > \frac{1}{p-1}$, we find that the zeros $s_0 \in \mathbb{Q}_p$ correspond bijectively to the zeros $T_0 \in \mathbb{Q}_p$, and for those zeros one has $T_0 \in p\mathbb{Z}_p$, $s_0 \in \mathbb{Z}_p$.

In general, the zeros T_0 of f_χ of course belong to an extension of $\mathbb{Q}_p(\theta)$ of degree $\leq \lambda_\chi$. Thus, if $\lambda_\chi = 1$, the unique zero T_0 is in $\mathbb{Q}_p(\theta)$. If $\theta = 1$ or θ is a quadratic character, this field is just $\mathbb{Q}_p$. For $\theta = 1$, λ_χ has been computed for all p below 12 million (see [1]); if nonzero, it is always $= 1$ and so the corresponding zero T_0 is in $p\mathbb{Z}_p$.

But also in the case $\lambda_\chi > 1$ there are numerous examples known in which f_χ has rational p-adic zeros T_0; see [3].

It will also be useful to introduce approximate zeros of $L_p(s,\chi)$. Let us call $\sigma \in \mathbb{Z}_p$ an *approximate zero of order* $l (\geq 1)$ for $L_p(s,\chi)$, if

$$L_p(\sigma,\chi) \equiv 0 \pmod{p^l}.$$

By [9], Theorem 5.12, rational p-adic integers σ_1 and σ_2 satisfy the condition

$$L_p(\sigma_1,\chi) \equiv L_p(\sigma_2,\chi) \pmod{p^l} \qquad \text{whenever} \qquad \sigma_1 \equiv \sigma_2 \pmod{p^{l-1}}. \tag{2.5}$$

Hence an approximate zero σ of order l is obtained by approximating a zero $s_0 \in \mathbb{Z}_p$ modulo p^{l-1}. Conversely, when does a given approximate zero σ really approximate some zero s_0? This question, related to Hensel's lemma, will play a role in Section 4.

3. Bernoulli numbers tending p-adically to zero

Throughout the following we use the abbreviations

$$\widehat{B}^m(\theta) = B^m(\theta)/m, \qquad \widetilde{B}^m(\theta) = (1-\theta(p)p^{m-1})\widehat{B}^m(\theta).$$

Theorem 3.1. *(i) Let $\sigma \in \mathbb{Z}_p$ be an approximate zero of order $l \geq 1$ for $L_p(s,\chi)$ and let*

$$\beta = \frac{1-t-\sigma}{p-1}\,(\in \mathbb{Z}_p).$$

Then

$$\widehat{B}^{t+(p-1)r_n(\beta)}(\theta) \equiv 0 \pmod{p^{n+1}} \qquad (n = 0, \dots, l-1). \tag{3.1}$$

(ii) Conversely, let $\beta \in \mathbb{Z}_p$ and assume that the congruences (3.1) *hold true. Then $\sigma = 1 - (t + (p-1)\beta)$ is an approximate zero of order l for $L_p(s, \chi)$.*

Proof. For any $n \geq 0$, let

$$w_n = t + (p-1)r_n(\beta) \ .$$

We have $\omega^{t-w_n} = 1$ and $\sigma \equiv 1 - w_n (\mathrm{mod}\ p^n)$. Hence, by (1.1) and (2.5),

$$\widetilde{B}^{w_n}(\theta) = -L_p(1-w_n, \chi) \equiv -L_p(\sigma, \chi) \pmod{p^{n+1}} \ .$$

This implies both parts of the theorem, with $\widetilde{B}$ in place of $\widehat{B}$. The assertions then follow, since $v_p(1-\theta(p)p^{w_n-1}) = 0$. One needs here the assumption that $t \geq 2$. ■

Note that the congruences (3.1) hold for all n in the range $0 \leq n \leq l-1$, once this congruence holds for $n = l-1$.

Theorem 3.1 implies that if $L_p(s, \theta\omega^t)$ $(2 \leq t \leq p)$ has an approximate zero of order 1, then

$$\widehat{B}^t(\theta) \equiv 0 \pmod{p} \ .$$

More generally, with the mere assumption that $\lambda_{\theta\omega^t} > 0$, it is known that one just has $v_p(\widehat{B}^t(\theta)) > 0$ (e.g., [8]).

By letting $l \to \infty$ in the preceding theorem we immediately get the following theorem.

Theorem 3.2. *(i) Let s_0 be a rational p-adic zero of $L_p(s, \chi)$ (hence $s_0 \in \mathbb{Z}_p$) and let*

$$\beta = \frac{1-t-s_0}{p-1} \ .$$

Then

$$\widehat{B}^{t+(p-1)r_n(\beta)}(\theta) \equiv 0 \pmod{p^{n+1}} \qquad (n = 0, 1, \dots). \tag{3.2}$$

(ii) Conversely, let $\beta \in \mathbb{Z}_p$ and assume that the congruences (3.2) *hold true. Then $s_0 = 1 - (t + (p-1)\beta) \in \mathbb{Z}_p$ is a zero of $L_p(s, \chi)$.*

For part (ii) of Theorem 3.2, we can replace the moduli p^{n+1} in (3.2) by any p^{z_n}, where the sequence (z_n) of rational numbers tends to infinity.

A by-product from part (i) of Theorem 3.2 is that the sequence $(r_n(\beta))$ tends to infinity in $\mathbb{Z}$, in other words, that β cannot be a nonnegative rational integer (under the given assumption). This is easy to prove directly, too.

Suppose, for a moment, that the value $t = p$ is reduced to $t = 1$. Then one obtains, with $\beta = -s_0/(p-1)$, the congruences

$$\widehat{B}^{1+(p-1)r_n(\beta)}(\theta) \equiv 0 \pmod{p^{n+1}} \qquad (n = 0, 1, \dots) \ ,$$

provided $v_p(1-\theta(p)) = 0$. If $v_p(1-\theta(p)) > 0$, these congruences are still valid for $n \geq n_0$, say, where n_0 is the least suffix such that $r_{n_0}(\beta) > 0$. Such an n_0 of course exists if $s_0 \neq 0$.

If $t = 1$ and $s_0 = 0$, then $w_n = 1$ for all $n \geq 0$ and the reasoning above produces nothing but the equation

$$(1-\theta(p))\widehat{B}^1(\theta) = 0, \tag{3.3}$$

which is equivalent to $\theta(p) = 1$. This is a well-known case in which λ_χ is "trivially" nonzero.

Now return to the original notation $2 \leq t \leq p$.

Example. Assume that $L_p(s,\chi)$ has the zero $s_0 = 0$. Then $\beta = (t-1)\sum_{j=0}^{\infty} p^j$ and $w_n = t + (t-1)(p^n - 1)$, so that the congruences in Theorem 3.2 become

$$\widehat{B}^{1+(t-1)p^n}(\theta) \equiv 0 \pmod{p^{n+1}} \qquad (n = 0, 1, \dots)\ .$$

In particular, if $t = p$, then the preceding discussion shows that $\theta(p) = 1$. In this case we can also derive these congruences directly by applying Kummer congruences to the trivial relation (3.3).

4. Strict uniqueness

Let s_1 and s_2 be two rational p-adic zeros of $L_p(s,\chi)$ with the corresponding β_1 and β_2, respectively, defined as in Theorem 3.2. Since $s_1 \neq s_2$ if and only if $\beta_1 \neq \beta_2$, we see that the preceding correspondence between different s_0 and the sequences $(r_n(\beta))$ satisfying (3.2) is bijective. In particular, if there is but one rational p-adic zero s_0 (not counting multiplicities), then the infinite sequence $(r_n(\beta))$ is unique.

In the case that $\lambda_\chi = 1$, the following stronger uniqueness result holds true.

Theorem 4.1. *Assume that $\lambda_\chi = 1$ and that $L_p(s,\chi)$ has an approximate zero σ of order $l \geq 2$ (or, alternatively, a rational p-adic zero s_0). If, for some n in the range $1 \leq n \leq l-1$ (or in the range $n \geq 1$, respectively),*

$$\widehat{B}^{t+(p-1)r_n}(\theta) \equiv 0 \pmod{p^{n+1}}, \qquad 0 \leq r_n < p^n\ ,$$

then $r_n = r_n(\beta)$ with β defined in Theorem 3.1 (or Theorem 3.2, respectively).

Proof. One has to show that r_n is unique mod p^n. By Theorem 3.1, it is enough to show that the congruence

$$L_p(\sigma,\chi) \equiv 0 \pmod{p^{n+1}}$$

determines σ uniquely mod p^n. Passing over to the Iwasawa power series we find, by (2.3) and (2.4), that this amounts to proving that the conditions

$$f_\chi(\tau) \equiv 0 \pmod{p^{n+1}}, \qquad \tau \equiv 0 \pmod{p} \tag{4.1}$$

determine τ uniquely mod p^{n+1}.

Since $\lambda_\chi = 1$, the derivative of f_χ satisfies

$$v_p(f'_\chi(\tau)) = v_p(a_1(\chi)) = 0 \, .$$

The assertion follows from this by the general principles of Newton's p-adic tangent method. Indeed, by writing

$$f_\chi(T) = (T-\tau)g(T) + f_\chi(\tau), \qquad g(T) \in \mathcal{O}_\theta[[T]] \, ,$$

we first have $f'_\chi(\tau) = g(\tau)$. If τ_0 satisfies the conditions (4.1), then $\tau_0 \equiv \tau (\mathrm{mod}\ p)$ and we obtain $0 = v_p(f'_\chi(\tau)) = v_p(g(\tau)) = v_p(g(\tau_0))$. The equation

$$f_\chi(\tau_0) = (\tau_0 - \tau)g(\tau_0) + f_\chi(\tau)$$

then yields $\tau_0 \equiv \tau (\mathrm{mod}\ p^{n+1})$. ■

As for the assumptions in Theorem 4.1, note that if $\mathbb{Q}_p(\theta) = \mathbb{Q}_p$, then the assumption $\lambda_\chi = 1$ implies that $L_p(s,\chi)$ has a rational p-adic zero.

Note a by-product from the preceding proof: Assume that $\lambda_\chi = 1$ and $L_p(s,\chi)$ has a rational p-adic zero s_0. If σ is an approximate zero of order $l \geq 2$ for $L_p(s,\chi)$, then

$$\sigma \equiv s_0 \pmod{p^{l-1}} \, .$$

In the case $\theta = 1$ Theorem 4.1 is essentially due to Kellner [4]. He also used it to compute (approximations of) zeros of $L_p(s,\omega^t)$.

5. Sharper divisibility

If $\lambda_\chi > 1$, it turns out that the congruences of Theorems 3.1 and 3.2 can be sharpened. This is a consequence of the following "sharper Kummer congruences".

Let δ denote the inverse of the ramification index of $\mathbb{Q}_p(\theta)/\mathbb{Q}_p$. Note that $0 < \delta \leq 1$; δ is the least positive v_p-value in the field $\mathbb{Q}_p(\theta)$.

Theorem 5.1. *If $\lambda_\chi > 1$, then*

$$\Delta_{\varphi(p^n)} \widetilde{B}^m(\theta) \equiv 0 \pmod{p^{n+\delta}}$$

for all $n \geq 1$ and all $m \equiv t (\mathrm{mod}\ p-1)$.

Proof. Fix n and m as in the theorem. From $\lambda_\chi > 1$ it follows ([8], Theorems 1 and 2) that

$$\Delta_{p-1}(\widetilde{B}^m(\theta)) \equiv 0 \pmod{p^{1+\delta}} \, .$$

By (2.1),

$$\Delta_{(p-1)p^{n-1}} \widetilde{B}^m(\theta) = p^{n-1} \Delta_{p-1} \widetilde{B}^m(\theta) + \sum_{k=2}^{p^{n-1}} \binom{p^{n-1}}{k} \Delta_{p-1}^k \widetilde{B}^m(\theta). \tag{5.1}$$

Here the first term on the right hand side is of v_p-value $\geq n+\delta$. So are also the remaining terms, since for k in the range $2 \leq k \leq p^{n-1}$ (for $n > 1$) one finds, making use of (2.2),

$$v_p\left(\binom{p^{n-1}}{k}\Delta_{p-1}^k \widetilde{B}^m(\theta)\right) = n-1-v_p(k)+v_p(\Delta_{p-1}^k \widetilde{B}^m(\theta)) \geq n-1-v_p(k)+k > n\,. \tag{5.2}$$

■

Theorem 5.2. *Assume that $\lambda_\chi > 1$. If $L_p(s,\chi)$ has an approximate zero $\sigma \in \mathbb{Z}_p$ of order $l \geq 2$, then*

$$\widehat{B}^{t+(p-1)r_n(\beta)}(\theta) \equiv 0 \pmod{p^{n+1+\delta}} \qquad (n = 0,\dots,l-2)\,,$$

where $\beta = \frac{1-t-\sigma}{p-1}$ as before. If $L_p(s,\chi)$ has a rational p-adic zero s_0, then the same congruences hold for all $n \geq 0$, with $\beta = \frac{1-t-s_0}{p-1}$.

Proof. As to the former part, we see from Theorem 3.1 that $\widetilde{B}^{t+(p-1)r_{n+1}(\beta)}(\theta) \equiv 0 \pmod{p^{n+2}}$ for $n = 0,\dots,l-2$. Theorem 5.1 then implies the assertion, first with $\widetilde{B}$ in place of $\widehat{B}$.

The latter part follows similarly from Theorem 3.2, or simply on letting $l \to \infty$ above. ■

If $\lambda_\chi > 1$ and $L_p(s,\chi)$ has a rational p-adic zero s_0, the preceding argument also shows that

$$\widehat{B}^{t+(p-1)r}(\theta) \equiv 0 \pmod{p^{n+\delta}} \qquad (n = 1,2,\dots)$$

for every $r \equiv r_{n-1}(\beta) (\mathrm{mod}\ p^{n-1})$. This result should be compared with Theorem 4.1. Recall that $\delta = 1$ when $\mathbb{Q}_p(\theta)/\mathbb{Q}_p$ is unramified.

To conclude, consider the case of χ mod p, that is, $\chi = \omega^t$, $t = 2,4,\dots,p-3$. In this case the last results imply the following corollary.

Corollary 5.1. *If $\lambda_{\omega^t} > 1$ and $L_p(s,\omega^t)$ has an approximate zero σ of order $l \geq 2$, then*

$$\widehat{B}^{t+(p-1)(r_n(\beta)+bp^n)} \equiv 0 \pmod{p^{n+2}} \qquad (n = 0,\dots,l-2), \tag{5.3}$$

where β is as above and b is any rational integer. In particular, for $l = 2$,

$$B^{t+p-1} \equiv B^t \equiv 0 \pmod{p^2}\,.$$

This result has a connection to the theory of cyclotomic fields. Let A_k denote the p-part of the ideal class group of the p^{k+1}th cyclotomic field ($k \geq 0$). By the Herbrand–Ribet theorem, the eigenspace of A_k corresponding to the character ω^{p-t} is nontrivial if and only if $\lambda_{\omega^t} > 0$. This condition is equivalent to $B^1(\omega^{t-1}) \equiv 0 (\mathrm{mod}\ p)$, or also to $B^t \equiv 0 (\mathrm{mod}\ p)$. Given that this is satisfied and assuming the

Vandiver conjecture, we know ([9], Corollary 10.17) that the eigenspace in question is cyclic of order p^{k+1} provided that

$$B^1(\omega^{t-1}) \not\equiv 0, \qquad \widehat{B}^t \not\equiv \widehat{B}^{t+p-1} \pmod{p^2}. \tag{5.4}$$

The latter incongruence fails if and only if $\lambda_{\omega^t} > 1$. Looking at the former incongruence, we first observe that

$$B^1(\omega^{t-1}) \equiv B^{(t-1)p^4+1} \equiv \widehat{B}^{(t-1)p+1} \pmod{p^2}$$

(for the first step, see, e.g., [8], Lemma 1). Hence $B^1(\omega^{t-1}) \equiv 0 (\mathrm{mod}\ p^2)$ is equivalent to

$$\widehat{B}^{t+(p-1)(t-1)} \equiv 0 \pmod{p^2}. \tag{5.5}$$

By Corollary 5.1, this congruence is valid if (1^o) $\lambda_{\omega^t} > 1$ and (2^o) $L_p(s, \omega^t)$ has an approximate zero σ of order 2. It follows from Theorem 3.1 that, conversely, (5.5) implies (2^o) (even without any assumption on λ_{ω^t}). But this can be seen directly, too: the choice $\sigma = 0$ works, since

$$L_p(0, \omega^t) = f_{\omega^t}(0) = -B^1(\omega^{t-1})$$

(cf. Example in Section 3).

Computations have shown (see [1]) that in the case $\lambda_{\omega^t} > 0$ the incongruences (5.4) as well as the incongruence $B^t \not\equiv 0 (\mathrm{mod}\ p^2)$ always hold in the range $p < 12 \cdot 10^6$.

Kellner ([4], p. 412) illustrates the congruences (5.3) by a graph, comparing it with his result corresponding to Theorem 4.1. He leaves open the question about the maximum value of n for which the congruences (5.3) hold true. From Corollary 5.1 and Theorem 3.1 we find that this maximum is $l - 2$, where l is the maximal order of the corresponding approximate zero of $L_p(s, \omega^t)$. In particular, the chain of congruences (5.3) is infinite exactly for every rational p-adic zero of $L_p(s, \omega^t)$.

Since these congruences express a rather strong condition in comparison to the one given by Kummer congruences, one may be tempted to suggest that they never occur, in other words, that the nonzero values of λ_{ω^t} are always $= 1$, at least in the presence of an approximate zero σ of high order. But one should be cautios, because in the more general case $\chi = \theta\omega^t$ it is well possible that $\lambda_\chi > 1$ and $L_p(s, \chi)$ has rational p-adic zeros, even for θ satisfying $\mathbb{Q}_p(\theta) = \mathbb{Q}_p$.

Here is one such example from [3] (p. S40). Let $p = 5$ and $\chi = \theta\omega^2$, where θ is the quadratic character mod 2504. Then $\lambda_\chi = 2$ and $L_p(s, \chi)$ has two rational p-adic zeros, approximately $s_1 = 2.41303$, $s_2 = 3.00334$ (in the usual 5-adic "decimal" notation). The Iwasawa power series in $\mathbb{Z}_5[[T]]$ is, with the accuracy given in [3],

$$f_\chi(T) = 0.010 + 0.00\,T + 1.3\,T^2 + 4\,T^3 + \cdots\ ,$$

and its zeros are approximately $T_1 = 0.331200$, $T_2 = 0.204143$.

For the size of λ_{ω^t}, see also Washington's heuristic discussion in [5], pp. 261–265.

6. The case $p = 2$

In the case $p = 2$ we take $\chi = \theta\omega^t$ with $t = 2$ or 3. Hence $\theta \neq 1$. The notation below is the same as in the case $p > 2$, unless stated otherwise.

We will apply Kummer's congruences modulo 2-powers in the following form:

$$\Delta_{2^h}^k (1 - \psi(2)2^{m-1})\widehat{B}^m(\psi) \equiv 0 \pmod{2^{(h+2)k+1}} \tag{6.1}$$

for all $k \geq 0$, $h \geq 1$, $m \geq 1$, provided the conductor of ψ is not a 2-power. These congruences, which are slightly stronger than those given in [6] (p. 239), are obtained from [7], formula (2), by induction on h, using the formula

$$\Delta_{2^h}^k = \sum_{i=0}^{k} \binom{k}{i} 2^{k-i} \Delta_{2^{h-1}}^{k+i}$$

(choose $c = 2^{h-1}$, $d = 2$ in the identity (2.1) of the present work). Note that the Iwasawa power series f_χ is two times the power series appearing in [7].

The function $L_2(s, \chi)$ is defined for $v_2(s) > -1$ and can be expressed by means of the Iwasawa power series in the form

$$L_2(s, \chi) = f_\chi((1 + 4d)^s - 1) \ .$$

This time we have $f_\chi(T) \in 2\mathcal{O}_\theta[[T]]$ and write

$$f_\chi(T) = 2\sum_{i=0}^{\infty} a_i(\chi)T^i \ .$$

The λ-invariant is again defined by $\lambda_\chi = \min\{\, i \geq 0 \mid v_2(a_i(\chi)) = 0\,\}$. In the disc $D_T = \{T \in \mathbb{C}_2 \mid v_2(T) > 0\}$ the function f_χ has λ_χ zeros (counting multiplicities). The zeros T_0 satisfying $v_2(T_0) > 1$ correspond bijectively to the zeros s_0 of $L_2(s, \chi)$; this correspondence is given by

$$T_0 = (1 + 4d)^{s_0} - 1, \qquad s_0 = \frac{\log(1 + T_0)}{\log(1 + 4d)} \ .$$

Thus, if $s_0 \neq 0$ (or, equivalently, $T_0 \neq 0$) then $v_2(s_0) = v_2(T_0) - 2$.

It follows that the rational 2-adic zeros s_0 correspond bijectively to the zeros $T_0 \in \mathbb{Q}_2$ satisfying $v_2(T_0) > 1$, and for those zeros one has $T_0 \in 4\mathbb{Z}_2$, $s_0 \in \mathbb{Z}_2$.

Approximate zeros of $L_2(s, \chi)$ satisfy the condition (2.5) in this case as well.

Theorem 6.1. *(i) Let $\sigma \in \mathbb{Z}_2$ be an approximate zero of order $l \geq 4$ for $L_2(s, \chi)$ and let*

$$\beta = \frac{1 - t - \sigma}{2} = \frac{b}{2} + \beta' \qquad (0 \leq b < 2,\ \beta' \in \mathbb{Z}_2) \ .$$

Then

$$\widehat{B}^{t+b+2r_n(\beta')}(\theta\omega^b) \equiv 0 \pmod{2^{n+4}} \qquad (n = 0, \ldots, l - 4). \tag{6.2}$$

(ii) Conversely, let $\beta = \frac{b}{2} + \beta'$ with $0 \leq b < 2$ and $\beta' \in \mathbb{Z}_2$, and assume that the congruences (6.2) *hold true. Then $\sigma = 1 - (t + 2\beta)$ is an approximate zero of order l for $L_2(s, \chi)$.*

Proof. Let $n \geq 3$. With $w_n = t + b + 2r_n(\beta') \in \mathbb{Z}$ we have $\omega^{t-w_n} = \omega^b$ and $\sigma = 1 - (t + b + 2\beta') \equiv 1 - w_n (\text{mod } 2^n)$. Hence

$$\widetilde{B}^{w_n}(\theta\omega^b) = -L_2(1 - w_n, \chi) \equiv -L_2(\sigma, \chi) \pmod{2^{n+1}}. \tag{6.3}$$

The Kummer congruences (6.1) for $k = 1$ and $h = n - 2$ show that

$$\widetilde{B}^{w_n}(\theta\omega^b) \equiv \widetilde{B}^{w_{n-3}}(\theta\omega^b) \pmod{2^{n+1}} .$$

It follows that $L_2(\sigma, \chi) \equiv 0 (\text{mod } 2^l)$ if and only if $\widetilde{B}^{w_{l-4}}(\theta\omega^b) \equiv 0 (\text{mod } 2^l)$. This proves the theorem. ■

Actually, (6.3) is valid for all $n \geq 0$. Thus one gets for approximate zeros of order $l = 1, 2$ or 3 congruences of the form of (6.2) but modulo lower 2-powers. In particular, if $L_2(s, \chi)$ has an approximate zero σ of order $l \geq 1$, we have

$$\text{either} \quad \widehat{B}^t(\theta) \equiv 0 \pmod{2^q} \qquad \text{or} \quad \widehat{B}^{t+1}(\theta\omega) \equiv 0 \pmod{2^q}$$

with $q = \min(l, 4)$, depending on whether or not $\beta = (1 - t - \sigma)/2$ is integral, respectively. A necessary and sufficient condition for this integrality is that $\sigma \equiv 1$ (mod 2) for $t = 2$ and $\sigma \equiv 0 (\text{mod } 2)$ for $t = 3$.

By contrast, the Kummer congruences (6.1) yield, for $k = 0$, that

$$\widehat{B}^m(\psi) \equiv 0 \pmod 2 \qquad (m = 2, 3, \dots) ,$$

whenever ψ is a character with conductor not a 2-power.

Theorem 6.2. *Theorem* 6.1 *holds true, when* σ *is replaced by a zero* $s_0 \in \mathbb{Z}_2$ *of* $L_2(s, \chi)$ *and in* (6.2) n *assumes all values* ≥ 0.

Proof. Let $l \to \infty$ in Theorem 6.1. ■

In the following, analogs of Theorems 4.1 and 5.2 are formulated for rational 2-adic zeros only; the corresponding discussion of approximate zeros is left to the reader.

Theorem 6.3. *Assume that* $\lambda_\chi = 1$, $L_2(s, \chi)$ *has a rational* 2*-adic zero* s_0 *and* $\beta = (1 - t - s_0)/2 \in \mathbb{Z}_2$. *If, for some* $n \geq 1$,

$$\widehat{B}^{t+2r_n}(\theta) \equiv 0 \pmod{2^{n+4}}, \qquad 0 \leq r_n < 2^n ,$$

then $r_n = r_n(\beta)$.

Proof. The proof is completely analogous to the proof of Theorem 4.1. ■

If $\lambda_\chi > 1$, then

$$\Delta_2 \widetilde{B}^m(\theta) \equiv 0 \pmod{2^{4+\delta}} \tag{6.4}$$

for all $m \equiv t (\mathrm{mod}\ 2)$; see [8], Theorems 1 and 2, where however the modulus is $2^{3+\delta}$ corresponding to a weaker version of (6.1)[1]. In the case that $\beta = (1-t-s_0)/2 \notin \mathbb{Z}_2$, we use this observation to formulate the following counterpart to Theorem 6.3 (with no obvious relation to λ_χ, however).

Theorem 6.4. *Assume that θ is a quadratic character and that $v_2(\Delta_2 \widetilde{B}^{t+1}(\theta\omega)) = 4$, $L_2(s,\chi)$ has a rational 2-adic zero s_0 and $\beta = (1-t-s_0)/2 = \frac{1}{2} + \beta'$ with $\beta' \in \mathbb{Z}_2$. If, for some $n \geq 1$,*

$$\widehat{B}^{t+1+2r_n}(\theta\omega) \equiv 0 \pmod{2^{n+4}}, \qquad 0 \leq r_n < 2^n ,$$

then $r_n = r_n(\beta')$.

Proof. The second assumption implies, by the Kummer congruences, that

$$v_2(\Delta_2 \widetilde{B}^m(\theta\omega)) = 4$$

for all $m \equiv t+1 (\mathrm{mod}\ 2)$.

Fix $n \geq 1$. The following formulas, for all $m \equiv t+1 (\mathrm{mod}\ 2)$, correspond to (5.1) and (5.2):

$$\Delta_{2^n} \widetilde{B}^m(\theta\omega) = \sum_{k=1}^{2^{n-1}} \binom{2^{n-1}}{k} \Delta_2^k \widetilde{B}^m(\theta\omega), \tag{6.5}$$

where

$$v_2\left(\binom{2^{n-1}}{k} \Delta_2^k \widetilde{B}^m(\theta\omega)\right) \begin{cases} = n+3 & \text{for } k=1, \\ > n+3 & \text{for } 2 \leq k \leq 2^{n-1}. \end{cases}$$

Hence

$$v_2(\Delta_{2^n} \widetilde{B}^m(\theta\omega)) = n+3 \tag{6.6}$$

whenever $m \equiv t+1 (\mathrm{mod}\ 2)$. By (6.2) and (6.1) we may write

$$\widetilde{B}^{t+1+2(r_{n-1}(\beta')+2^{n-1}u)}(\theta\omega) \equiv d_u 2^{n+3} \pmod{2^{n+4}},$$

with $v_2(d_u) \geq 0$, for all $u \geq 0$. Again by (6.1),

$$\Delta_{2^n}^2 \widetilde{B}^m(\theta\omega) \equiv 0 \pmod{2^{n+4}}$$

(even mod 2^{2n+5}) for all $m \geq 1$. By taking $m = t+1+2(r_{n-1}(\beta') + 2^{n-1}u)$ we obtain from this that $\Delta^2 d_u \equiv 0 (\mathrm{mod}\ 2)$. Therefore,

$$d_u \equiv d_0 + u(d_1 - d_0) \pmod 2 \qquad (u = 0, 1, \dots) .$$

Eq. (6.6) shows that $d_0 \not\equiv d_1 (\mathrm{mod}\ 2)$. Hence there is a unique $u = u_0 \in \{0,1\}$ such that $d_{u_0} \equiv 0 (\mathrm{mod}\ 2)$, that is,

$$\widetilde{B}^{t+1+2(r_{n-1}(\beta')+2^{n-1}u_0)}(\theta\omega) \equiv 0 \pmod{2^{n+4}} .$$

This congruence is equivalent to the one in which $\widetilde{B}$ is replaced by $\widehat{B}$. Thus the theorem follows from the uniqueness of u_0. ■

[1] Note an error in [8] in the statement of Theorem 2: when $p = 2$, the congruence $n \equiv t (\mathrm{mod}\ p-1)$ should read $n \equiv t (\mathrm{mod}\ 2)$.

The method of this proof could also be used to provide an alternative proof for Theorems 4.1 and 6.3.

The following results correspond to Theorems 5.1 and 5.2.

Theorem 6.5. *If* $\lambda_\chi > 1$, *then*

$$\Delta_{2^n} \widetilde{B}^m(\theta) \equiv 0 \pmod{2^{n+3+\delta}}$$

for all $n \geq 1$ *and all* $m \equiv t \pmod 2$.

Proof. Use (6.5), with $\theta\omega$ replaced by θ, together with (6.4) and the Kummer congruences. ■

Theorem 6.6. *Assume that* $\lambda_\chi > 1$. *If* $L_2(s,\chi)$ *has a rational* 2*-adic zero* s_0 *and* $\beta = (1-t-s_0)/2 \in \mathbb{Z}_2$, *then*

$$\widehat{B}^{t+2r_n(\beta)}(\theta) \equiv 0 \pmod{2^{n+4+\delta}} \qquad (n = 0, 1, \dots). \tag{6.7}$$

Proof. Theorem 6.2 implies that $\widetilde{B}^{t+2r_{n+1}(\beta)}(\theta) \equiv 0 \pmod{2^{n+5}}$. The assertion then follows by virtue of the preceding theorem. ■

To compare this result with Theorem 6.3 it is illuminating to write down a consequence from (6.7) in the form

$$\widehat{B}^{t+2(r_{n-1}(\beta)+2^{n-1}b)}(\theta) \equiv 0 \pmod{2^{n+3+\delta}} \qquad (n = 1, 2, \dots)\ ,$$

where b is any rational integer.

References

[1] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, M.A. Shokrollahi, *Irregular primes and cyclotomic invariants to 12 million*, J. Symbolic Comput. **31** (2001), 89–96.

[2] L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine Angew. Math. **202** (1959), 174–182.

[3] R. Ernvall, T. Metsänkylä, *Computation of the zeros of p-adic L-functions*, Math. Comp. **58** (1992), 815–830, S37–S53.

[4] B. Kellner, *On irregular prime power divisors of the Bernoulli numbers*, Math. Comp. **76** (2007), 405–441.

[5] S. Lang, *Cyclotomic Fields I and II*, combined 2nd ed., Springer-Verlag, New York, 1990.

[6] H. W. Leopoldt, *Eine p-adische Theorie der Zetawerte, II: Die p-adische* Γ*-Transformation*, J. Reine Angew. Math. **274**/**275** (1975), 224–239.

[7] T. Metsänkylä, *Note on certain congruences for generalized Bernoulli numbers*, Arch. Math. (Basel) **30** (1978), 595–598.

[8] T. Metsänkylä, *Iwasawa invariants and Kummer congruences*, J. Number Theory **10** (1978), 510–522.
[9] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer-Verlag, New York, 1997.

Address: Department of Mathematics, University of Turku, FI-20014 Turku, Finland
E-mail: taumets@utu.fi
Received: 13 December 2007