Journal of Number Theory **69**, 50–61 (1998)
Article No. NT972195

# $p$-Adic $L$-Functions and Sums of Powers

Lawrence C. Washington

*Department of Mathematics, University of Maryland, College Park, Maryland 20742*

*Communicated by A. Granville*

Received November 25, 1996; revised May 15, 1997

We give an explicit $p$-adic expansion of $\sum_{j=1,\,(j,\,p)=1}^{np} j^{-r}$ as a power series in $n$. The coefficients are values of $p$-adic $L$-functions. © 1998 Academic Press



Several authors (see [2, pp. 95–103]) have studied the sums

$$\sum_{\substack{j=1\\(j,\,p)=1}}^{np} \frac{1}{j^r}$$

modulo powers of the prime $p$, especially in the cases where $r=1$ or $n=1$. In the present paper, we give explicit $p$-adic expansions of these sums as power series in $n$. This result was inspired by a recent paper of D. Boyd [1], who gave such an expansion in the case $r=1$. An examination of his proof shows that the coefficients of the expansion are values of $p$-adic $L$-functions. In the following, we give another proof of Boyd's result and show that there is such an expansion for each integer $r$. This yields several classical congruences.

Let $p$ be a prime and let $L_p(s,\chi)$ be the $p$-adic $L$-function attached to a character $\chi$ (we give relevant facts about $p$-adic $L$-functions below). Let $\omega$ be the Teichmüller character. Our main result is the following.

Theorem 1. *Let $p$ be an odd prime and let $n \geqslant 1$ and $r$ be integers.*

(a) *If $r \geqslant 1$, then*

$$\sum_{\substack{j=1\\(j,\,p)=1}}^{np} \frac{1}{j^r} = -\sum_{k=1}^{\infty} \binom{-r}{k} L_p(r+k,\omega^{1-k-r})(pn)^k$$



0022-314X/98 $25.00

*and*

$$\sum_{\substack{j=1\\(j,2)=1}}^{2n} \frac{1}{j^r} = -\sum_{k=1}^{\infty} \binom{-r}{k} L_2(r+k, 1)(2n)^k.$$

(b) *If* $r \geqslant 0$, *then*

$$\sum_{\substack{j=1\\(j,p)=1}}^{np} j^r = \frac{1}{r+1}\left(1-\frac{1}{p}\right)(pn)^{r+1} - \sum_{\substack{k=1\\k\neq r+1}}^{\infty} \binom{r}{k} L_p(-r+k, \omega^{1-k+r})(pn)^k$$

*and*

$$\sum_{\substack{j=1\\(j,2)=1}}^{2n} j^r = \frac{1}{r+1}\left(1-\frac{1}{2}\right)(2n)^{r+1} - \sum_{\substack{k=1\\k\neq r+1}}^{\infty} \binom{r}{k} L_2(-r+k, 1)(2n)^k.$$

*Remarks.* (1) The case $r=1$ in the first formula is easily shown to be equivalent to Boyd's result.

(2) The sums in (b) are finite ($k \leqslant r$) and are simply variations of the classical formula for sums of powers in terms of Bernoulli polynomials. The omitted term for $k=r+1$ is

$$\binom{r}{r+1} L_p(1, \omega^0)(pn)^{r+1} = 0 \cdot \infty,$$

since the $p$-adic zeta function has a pole at 1. If we interpret this term to be

$$\lim_{s\to r} \binom{s}{r+1} L_p(s+1-r, \omega^0)(pn)^{r+1} = \frac{-1}{r+1}\left(1-\frac{1}{p}\right)(pn)^{r+1},$$

then the second equation is the same as the first. This of course is not surprising since the various expressions are $p$-adically continuous (except for poles) in $r$ if $r$ is restricted to a fixed residue class mod $p-1$.

(3) The value of the $p$-adic $L$-function $L_p(s, \omega^t)$ at the negative integer $1-m$ equals $(1-\omega^{t-m}(p)\, p^{m-1})\, L(1-m, \omega^{t-m})$, where the last factor is the classical Dirichlet $L$-function for the character $\omega^{t-m}$ (under a suitable embedding of $\omega$ into $\mathbb{C}$). The terms in the sums all correspond to the case where $t-m=0$ (though sometimes with $1-m>0$), which means the character $\omega$ "disappears" and we are working with $p$-adic analogues of values of the Riemann $\zeta$-function.

(4) The above is the $p$-adic analogue of the easily proved identity

$$\sum_{j=1}^{\infty}\left(\frac{1}{j^r}-\frac{1}{(j+x)^r}\right)=-\sum_{k=1}^{\infty}\binom{-r}{k}\zeta(r+k)\,x^k,$$

which holds for $r\geqslant 1$. If we could choose $x$ to be a positive integer, we would get a partial sum on the left; but the right side does not converge for $|x|\geqslant 1$. There is an analogue of the second equation in Theorem 1 for non-negative integers $x$, but it is again simply the expression for sums of powers in terms of Bernoulli polynomials. We also can remove the multiples of $p$ from the sum and obtain

$$\sum_{\substack{j=1\\(j,p)=1}}^{\infty}\left(\frac{1}{j^r}-\frac{1}{(j+x)^r}\right)=-\sum_{k=1}^{\infty}\binom{-r}{k}(1-p^{-(r+k)})\,\zeta(r+k)\,x^k.$$

As pointed out above, the values of the $p$-adic $L$-functions in the theorem are analogues of the numbers $(1-p^{-(r+k)})\,\zeta(r+k)$.

The theorem contains several classical results. As examples, we give the following three results of Glaisher ([4, 5]; see also [7]). The first part of Corollary 1 with $r=1$ implies Wolstenholme's theorem [6]. All of these Corollaries result from looking at the first non-zero term in Theorem 1 ($k=2$ if $r$ is odd, $k=1$ if $r$ is even). The special case in Corollary 3 corresponds to the leading term being a $p$-adic $L$-function with a pole. The other case where the leading term has a pole yields the trivial result that $\sum_{j=1}^{p-1} 1/j^{p-1}\equiv -1 \pmod{p}$.

Of course, using more terms in Theorem 1 yields stronger congruences. It is possible to use part (b) of Theorem 1 to obtain congruences for sums of positive powers, though these are easily (and equivalently) obtained using Bernoulli polynomials.

Corollary 1. *Let $r\geqslant 1$ be odd and suppose $p\geqslant r+4$. Then*

$$\sum_{j=1}^{p-1}\frac{1}{j^r}\equiv -\frac{r(r+1)}{2(r+2)}B_{p-r-2}\,p^2 \pmod{p^3}.$$

Corollary 2. *Let $r\geqslant 2$ be even and suppose $p\geqslant r+3$. Then*

$$\sum_{j=1}^{p-1}\frac{1}{j^r}\equiv \frac{r}{r+1}B_{p-r-1}\,p \pmod{p^2}.$$

COROLLARY 3.

$$\sum_{j=1}^{p-1} \frac{1}{j^{p-2}} \equiv -p \qquad (\mathrm{mod}\ p^2).$$

We can also give information on when a higher power of $p$ divides these sums.

COROLLARY 4. *If $r$ is odd, $1 \leqslant r \leqslant p-6$, and $L_p(s, \omega^{-1-r})$ has a zero $\beta$ with $\beta \equiv r+2 \pmod p$, then*

$$\sum_{j=1}^{p-1} \frac{1}{j^r} \equiv 0 \qquad (\mathrm{mod}\ p^4).$$

*If $r$ is even, $2 \leqslant r \leqslant p-5$, and $L_p(s, \omega^{-r})$ has a zero $\beta$ with $\beta \equiv r+1 \pmod p$, then*

$$\sum_{j=1}^{p-1} \frac{1}{j^r} \equiv 0 \qquad (\mathrm{mod}\ p^3).$$

The converse of Corollary 4 is not necessarily true. It is possible, though probably rare, that these higher congruences hold without the existence of a zero. This problem can be interpreted in terms of the coefficients of the corresponding Iwasawa power series (see the remark after the proof of Corollary 4).

In Theorem 2 below, we treat sums over arithmetic progressions, from which it is also possible to obtain results such as Theorem 1 and the above corollaries for sums of the form

$$\sum_{\substack{j=1 \\ (j,\, p)=1}}^{nF} \chi(j)\, j^{\pm r},$$

where $\chi$ is a Dirichlet character and $F$ is any multiple of $p$ and the conductor of $\chi$. In particular, the following holds:

If $\chi \neq 1$ and $r \in \mathbb{Z}$, then

$$\sum_{\substack{j=1 \\ (j,\, p)=1}}^{nF} \frac{\chi(j)}{j^r} = - \sum_{\substack{k=1 \\ k \neq -r+1}}^{\infty} \binom{-r}{k} (nF)^k\, L_p(r+k, \chi\omega^{1-r-k}).$$

# 1. $p$-ADIC $L$-FUNCTIONS

Before giving the proofs, we need a few facts about $p$-adic $L$-functions. Define the Bernoulli numbers by the series

$$\frac{t}{e^t-1}=\sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Let $\omega$ be the $p$-adic-valued Teichmüller character, so $\omega(a)\equiv a \pmod p$ and $\omega(a)^p=\omega(a)$ when $p\geqslant 3$. If $p\nmid a$, let $\langle a\rangle=a/\omega(a)$. Finally, if $x\in\mathbb{Z}_p$ ($=$the $p$-adic integers), let $\binom{x}{k}=(x)(x-1)\cdots(x-k+1)/k!$. When $p$ is odd, or when $p=2$ and $\omega^t=1$, the $p$-adic $L$-function for the character $\omega^t$ (this is the only case we need) satisfies

$$L_p(s,\omega^t)=\frac{1}{s-1}\frac{1}{p}\sum_{a=1}^{p-1}\omega(a)^t\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{p}{a}\right)^j$$

for $s\in\mathbb{Z}_p$. This is a $p$-adic analytic function (except possibly at $s=1$) and has the following properties:

(1) $L_p(1-k,\omega^t)=-(1-p^{k-1})\,B_k/k$ when $1\leqslant k\equiv t \pmod{p-1}$

(2) $L_p(s,\omega^t)$ is identically 0 when $t$ is odd

(3) $L_p(s,\omega^t)\in\mathbb{Z}_p$ for all $s\in\mathbb{Z}_p$ when $t\not\equiv 0 \pmod{p-1}$

(4) If $t\not\equiv 0 \pmod{p-1}$, then $L_p(s_1,\omega^t)\equiv L_p(s_2,\omega^t) \pmod p$ for all $s_1, s_2\in\mathbb{Z}_p$

(5) $L_p(s,1)$ has a simple pole at $s=1$ with residue $1-1/p$.

The proofs of (1)–(5) may be found in [8, Chap. 5]. The formula for $L_p(s,\omega^t)$ is also proved there, except for the case of $p=2$, where usually the sum is for $a=1, 3$ and an extra factor of 2 is introduced in order to obtain an expression that is analytic for all $s\in\mathbb{C}_2$ with $|s|\leqslant 2^{3/2}$. However, if we restrict to $s\in\mathbb{Z}_2$, the above formula is a uniformly convergent sum of continuous functions on $\mathbb{Z}_2$ and takes on the correct values at negative integers (by the proof in [8]; the problem with general $s$ is that the binomial coefficients can have negative 2-adic valuation when $s$ lies in an extension of $\mathbb{Z}_2$). Therefore the formula must give the desired function $L_2(s,1)$. The case with $p=2$ and $t=1$, where the function is identically 0, clearly cannot be given by this formula since we would obtain the same function as when $t=0$.

Let $F$ be a positive integer and let $0<a<F$. Define the partial zeta function (for $\mathrm{Re}(s)>1$) by

$$H(s,a,F)=\sum_{n=0}^{\infty}\frac{1}{(a+nF)^s}.$$

It is known that $H(s, a, F)$ can be analytically continued to the whole complex plane, except for a simple pole at $s = 1$ with residue $1/F$, and

$$H(1-k, a, F) = -\frac{F^{k-1}}{k} B_k\left(\frac{a}{F}\right)$$

for positive integers $k$, where $B_k(X)$ is the $k$th Bernoulli polynomial.

When $F$ is a multiple of $p$ and $(a, p) = 1$, there is a $p$-adic analogue defined by

$$H_p(s, a, F) = \frac{1}{s-1} \frac{1}{F} \langle a \rangle^{1-s} \sum_{j=0}^{\infty} \binom{1-s}{j} (B_j) \left(\frac{F}{a}\right)^j$$

for $s \in \mathbb{Z}_p$. It satisfies

$$H_p(1-k, a, F) = \omega^{-k}(a)\, H(1-k, a, F)$$

for all positive integers $k$, and it has a simple pole at $s = 1$ with residue $1/F$. This is proved in [8, Theorem 5.9], except in the case $p = 2$, where it is required that $4 \mid F$. This extra condition is not needed if we restrict to $s \in \mathbb{Z}_p$, as discussed above. Note that

$$L_p(s, \omega^t) = \sum_{a=1}^{p-1} \omega^t(a)\, H_p(s, a, F),$$

except in the case where $p = 2$ and $\omega^t = \omega$.

We shall actually prove the following result. Taking $F = p$ and summing over $1 \leqslant a \leqslant p-1$ yields Theorem 1.

THEOREM 2. *Let $F$ be a multiple of $p$ and let $(a, p) = 1$. If $r \geqslant 1$ then*

$$\sum_{\ell=0}^{n-1} \frac{1}{(\ell F + a)^r} = -\sum_{k=1}^{\infty} \binom{-r}{k} \omega(a)^{1-r-k} H_p(r+k, a, F)(Fn)^k.$$

*If $r \geqslant 0$ then*

$$\sum_{\ell=0}^{n-1} (\ell F + a)^r$$

$$= \frac{1}{r+1} \frac{1}{F} (Fn)^{r+1} - \sum_{\substack{k=1 \\ k \neq r+1}}^{\infty} \binom{r}{k} \omega(a)^{1+r-k} H_p(-r+k, a, F)(Fn)^k.$$

## 2. THE PROOFS

*Proof of Theorem* 2. We need the following identity on binomial coefficients:

$$\frac{1}{r+k-1}\binom{-r}{k}\binom{1-r-k}{j}=\frac{-1}{k+j}\binom{-r}{k+j-1}\binom{k+j}{j}.$$

This holds for all integers $r$, $j$, $k$ with $j, k \geqslant 0$, $j+k>0$, and $r \neq 1-k$.

We also need the classical fact that, for positive integers $s$ and $n$,

$$\sum_{\ell=0}^{n-1} \ell^{s-1}=\frac{1}{s}\sum_{j=0}^{s-1}\binom{s}{j}(B_j)\, n^{s-j}.$$

Let $r \geqslant 1$. Then

$$\begin{aligned}
&\sum_{k=1}^{\infty}\binom{-r}{k}\omega(a)^{1-r-k} H_p(r+k, a, F)(Fn)^k\\
&=\sum_{k=1}^{\infty}\sum_{j=0}^{\infty}\binom{-r}{k}\frac{1}{F(r+k-1)}a^{1-r-k}\binom{1-r-k}{j}B_j\left(\frac{F}{a}\right)^j(Fn)^k\\
&=-\sum_{k=1}^{\infty}\sum_{j=0}^{\infty}\frac{1}{F}\binom{-r}{k+j-1}\binom{k+j}{j}\frac{1}{k+j}B_j n^k\left(\frac{F}{a}\right)^{j+k}a^{1-r}\\
&=-\sum_{s=1}^{\infty}\sum_{j=0}^{s-1}\frac{1}{F}\binom{-r}{s-1}\binom{s}{j}\frac{1}{s}B_j n^{s-j}\left(\frac{F}{a}\right)^s a^{1-r}\\
&=-\sum_{s=1}^{\infty}a^{-r}\left(\frac{F}{a}\right)^{s-1}\binom{-r}{s-1}\sum_{\ell=0}^{n-1}\ell^{s-1}\\
&=-\sum_{\ell=0}^{n-1}a^{-r}\sum_{s=1}^{\infty}\binom{-r}{s-1}\left(\frac{F\ell}{a}\right)^{s-1}\\
&=-\sum_{\ell=0}^{n-1}\frac{1}{(F\ell+a)^r}.
\end{aligned}$$

The proof of the second equation is similar: Allow $r \leqslant 0$ in the above and omit the terms with $k=-r+1$, or equivalently the terms with $j=r+s-1$ and $s \geqslant 1-r$. The expression $\sum_{\ell=0}^{n-1}\ell^{s-1}$ must be changed to

$$\sum_{\ell=0}^{n-1}\ell^{s-1}-\frac{1}{s}B_{r+s-1}n^{1-r}\binom{s}{r+s-1}$$

when $s \geqslant 1-r$ to account for the omitted terms. Since $\binom{-r}{s-1}=0$ for $s \geqslant 2-r$, we only have to make this correction for the term corresponding to $s=1-r$. An easy calculation yields the result. ∎

The corollaries result from looking at the first nonzero term in the sum in Theorem 1. To do this, we first need to treat the higher terms.

LEMMA. *Assume* $p \geqslant 5$, $p \geqslant r$, *and* $k \geqslant 3$. *If either* $r \neq p-3$ *or* $k \neq 3$, *then* $L_p(r+k, \omega^{1-k-r})\, p^k \equiv 0 \pmod{p^3}$. *In the case* $r = p-3$ *and* $k = 3$, *we have* $L_p(p, 1)\, p^3 \equiv p^2 \pmod{p^3}$.

*Proof.* If $1-k-r \not\equiv 0 \pmod{p-1}$ then $v_p(L_p(r+k, \omega^{1-k-r})) \geqslant 0$, so we may restrict to the case $1-k-r \equiv 0 \pmod{p-1}$. For $j \geqslant 1$ we may write

$$\frac{1}{s-1}\binom{1-s}{j} = \frac{-1}{j}\binom{-s}{j-1},$$

so the contribution to the denominator from this factor is bounded by $j$. Since the von Staudt–Clausen theorem implies that at most $p^1$ divides the denominator of the Bernoulli numbers, we obtain

$$L_p(s, 1) \equiv \frac{1}{s-1}\frac{1}{p}\sum_{a=1}^{p-1} \langle a \rangle^{1-s} \qquad (\mathrm{mod}\ \mathbb{Z}_p).$$

Therefore, since $\langle a \rangle \equiv 1 \pmod{p}$,

$$v_p(L_p(s, 1)) = -v_p(s-1) - 1.$$

Since (with $\log_p$ denoting the usual archimedean logarithm to the base $p$)

$$v_p(r+k-1) + 1 < \log_p(k+p) + 1 < k-2$$

for $k \geqslant 5$, we only need to consider $k = 3$ and $k = 4$.

For $k = 3$, if $r+k-1 \equiv 0 \pmod{p-1}$, then $r = p-3$, so we are in the exceptional case in the statement of the lemma. We have $L_p(p, 1) \equiv (1/(p-1))((p-1)/p) \equiv (1/p) \pmod{\mathbb{Z}_p}$, which yields the result in this case. When $k = 4$, we have $r = p-4$ and $v_p(L_p(p, 1)\, p^4) = -1+4 = 3$. ∎

*Proof of Corollary* 1. Since $r$ is odd, the summand for $k = 1$ vanishes in Theorem 1. From the lemma we obtain

$$\begin{aligned}
\sum_{j=1}^{p-1} \frac{1}{j^r} &\equiv -\frac{r(r+1)}{2} L_p(r+2, \omega^{-1-r})\, p^2 \\
&\equiv -\frac{r(r+1)}{2} L_p(r+2-p+1, \omega^{-1-r})\, p^2 \\
&\equiv \frac{r(r+1)}{2}(1 - p^{p-r-3})\frac{B_{p-r-2}}{p-r-2}\, p^2 \\
&\equiv -\frac{r(r+1)}{2(r+2)} B_{p-r-2}\, p^2 \qquad \pmod{p^3}. \quad ∎
\end{aligned}$$

*Proofs of Corollaries* 2 *and* 3. Similar to the proof of Corollary 1. For Corollary 3, we need the special case of the above lemma. ∎

*Proof of Corollary* 4. We consider the case of odd $r$. The case of even $r$ is similar. The terms for $k=1$ and $k=3$ vanish identically. Since $r \neq p-4$, the argument in the proof of the lemma shows that the terms with $k \geqslant 4$ are $\equiv 0 \pmod{p^4}$. Therefore

$$\sum_{j=1}^{p-1} \frac{1}{j^r} \equiv -\binom{-r}{2} L_p(r+2, \omega^{-1-r})\, p^2 \qquad \pmod{p^4}.$$

It follows easily from [8, Theorem 5.12] that if $s_1 \equiv s_2 \pmod{p}$ then $L_p(s_1, \omega^{-1-r}) \equiv L_p(s_1, \omega^{-1-r}) \pmod{p^2}$ (the congruence also follows from the expression of the $p$-adic $L$-function in terms of its Iwasawa power series). Therefore

$$L_p(r+2, \omega^{-1-r}) \equiv L_p(\beta, \omega^{-1-r}) = 0 \qquad \pmod{p^2},$$

which yields the result. ∎

*Remark.* Let $f(T, \omega^{-1-r}) = a_0 + a_1 T + \cdots \in \mathbb{Z}_p[[T]]$ be the Iwasawa power series, so $L_p(s, \omega^{-1-r}) = f((1+p)^s - 1, \omega^{-1-r})$. If $p \mid a_1$, we have $L_p(s_1, \omega^{-1-r}) \equiv L_p(s_2, \omega^{-1-r}) \pmod{p^2}$ for all $s_1, s_2 \in \mathbb{Z}_p$, so we only need the existence of $\beta$, rather than the congruence $\beta \equiv r+2 \pmod{p}$, to obtain Corollary 4. Of course, the existence of $\beta$ implies $p \mid a_0$. There are no known examples with both $p \mid a_0$ and $p \mid a_1$.

## 3. DIVISIBILITY BY $p$

Boyd's result was introduced to study the question of when a prime $p$ divides the partial sums of the harmonic series. Let

$$H_n^r = \sum_{j=1}^{n} \frac{1}{j^r}$$

and let

$$S_p^r = \{n \mid p \text{ divides the numerator of } H_n^r\}.$$

Boyd gave a heuristic argument based on branching processes that indicated that $S_p^1$ should be finite for each $p$. For a set of primes of density $1/e$, $S_p^1$ should consist of only the three numbers $p$, $p^2-p$, and $p^2-1$. However, there should be $p$ for which $S_p^1$ is arbitrarily large. For example, he was able to show that $S^1_{11}$ has 638 elements. This required a lot of computation, and the expansion of Theorem 1 as a power series in $n$ was very useful.

When $r \geqslant 2$, the situation is somewhat different. We give a crude probability argument that indicates what should be expected. From Theorem 1, we have (if $p \geqslant r+3$)

$$H^r_{pn} - \frac{1}{p^r} H^r_n \equiv 0 \pmod{p}.$$

Also, it is easy to see that, for $0 \leqslant k \leqslant p-1$,

$$H^r_{pn+k} \equiv H^r_{pn} + H^r_k \pmod{p}.$$

It follows that, for $0 \leqslant k \leqslant p-1$,

$$H^r_{pn+k} \equiv 0 \pmod{p} \quad \Leftrightarrow \quad H^r_n \equiv 0 \pmod{p^r} \quad \text{and} \quad H^r_{pn} \equiv -H^r_k \pmod{p}$$

(see [1], [3]).

For simplicity, consider the case $r=3$. We regard $H^3_k$ for $0 \leqslant k \leqslant p-2$ as random mod $p^3$, and also $H^3_{p-1}/p^2$ as random mod $p$ (cf. Corollary 1). These heuristic assumptions are of course unproved, but it seems reasonable to expect that they are approximately true. For the numbers $H^3_a$ with $1 \leqslant a \leqslant p-1$, the standard heuristic argument (see the corresponding argument for Bernoulli numbers in [8, p. 63]) would say that with probability $e^{-1}/j!$ the number of $a$ with $H^3_a \equiv 0 \pmod{p}$ should be $j+1$ (the "$+1$" occurring because we know that $H^3_{p-1} \equiv 0 \pmod{p}$); but this ignores the fact that $H^3_a \equiv H^3_{p-1-a} \pmod{p}$. If we regard this as being the only relation that is not random, then we get $2j+1$ with probability $e^{-1/2}(1/2)^j/j!$ (the contribution of the midpoint $a=(p-1)/2$ is negligible).

Now consider a number $a+bp$ with $0 \leqslant a$, $b \leqslant p-1$, $b \neq 0$. We have $H^3_{a+bp} \equiv 0 \pmod{p}$ if and only if $H^3_b \equiv 0 \pmod{p^3}$ and $H^3_{bp} \equiv -H^3_a \pmod{p}$. When $1 \leqslant b \leqslant p-2$, this happens with probability $1/p^4$. Since we have (slightly less than) $p^2$ such numbers $a+bp$, the probability that at least one of them yields an example of $H^3_{a+bp} \equiv 0 \pmod{p}$ is approximately $1-(1-1/p^4)^{p^2} \sim 1/p^2$. Since $\sum_p 1/p^2 < \infty$, we expect only finitely many $p$ to contribute examples. For $b=p-1$, we have $H^3_{p-1} \equiv 0 \pmod{p^3}$ with probability $1/p$. When this happens, we look at the congruence $H^3_{(p-1)p} \equiv -H^3_a \pmod{p}$. This congruence is satisfied for $2k$ values of $a$ with probability $e^{-1/2}(1/2)^k/k!$ (recall that $H^3_{p-1-a} \equiv H^3_a$; we ignore $a=(p-1)/2$). Since $\sum_p 1/p = \infty$, we expect infinitely many $p$ to yield examples, though such $p$ should be rare. In fact, Corollary 1 says that these $p$ must satisfy $B_{p-5} \equiv 0 \pmod{p}$. In summary, we expect a thin set of $p$ for which there exists some $a \leqslant p-1$ with $H^3_{a+(p-1)p} \equiv 0 \pmod{p}$, and otherwise, except for finitely many exceptional $p$, the only cases with $H_n^3 \equiv 0 \pmod{p}$ should have $n \leqslant p-1$. A slight extension of this argument shows that we do not expect $S_p^3$ to contain any $n > p^2$, except possibly for finitely many exceptional $p$. However, the contributions of the numbers $a + p(p-1)$ indicates that $S_p^3$ can contain arbitrarily large sets of integers between $p$ and $p^2$.

For $r \geqslant 4$, a similar argument shows that we should not expect $S_p^r$ to contain any $n > p$. For $r = 2$, we do not expect $S_p^2$ to contain any $n > p^2$, but there should be a thin set of $p$ where $S_p^2$ contains at least one $n$ with $p < n < p^2$.

Of course, the above arguments are rather imprecise. For example, they do not take into account various relations among the numbers $H_k^r$. However, such relations should have a minimal effect on the heuristics.

For $r = 3$, and $7 \leqslant p < 200$, there are 27 values of $p$ for which $S_p^3 = \{p-1\}$. For 11 values of $p$, $S_p^3$ has 3 elements. For 4 primes $p$, $S_p^3$ has 5 elements, and $S_{37}^3$ has 7 elements.

The prime $p = 37$ is an interesting example. A calculation shows that $H_k^3 \equiv 0 \pmod{37}$ for $k = 4$, 13, 23, 32, 36, and $H_k^3 \not\equiv 0 \pmod{37^3}$ for $k = 4$, 13, 23, 32. We have $B_{37-5} \equiv 0 \pmod{37}$, so $H_{36}^3 \equiv 0 \pmod{37^3}$. A calculation yields $H_{36}^3/37^3 \equiv 28 \pmod{37}$. For $k = 8$ and $k = 28$, we have $H_k^3 \equiv 9 \pmod{37}$, so $H_{36*37+k}^3 \equiv 0 \pmod{37}$ for these two values of $k$. Neither of these two values of $H$ is divisible by $37^3$, so we cannot continue further. Therefore 37 divides $H_k^3$ for precisely the values $k = 4$, 13, 23, 32, 36, 1340, 1360.

## ACKNOWLEDGMENTS

The author thanks David Boyd for suggesting that [1] had some relation to $p$-adic $L$-functions. The author thanks the Institute for Advanced Study for its hospitality during the preparation of this paper. This research was partially supported by a grant from NSA.

## REFERENCES

1. D. Boyd, A $p$-adic study of the partial sums of the harmonic series, *Experiment. Math.* **3** (1994), 287–302.
2. L. E. Dickson, “History of the Theory of Numbers,” Vol. I, Chelsea, New York, 1952 (especially Chapter 3).
3. A. Eswarathasan and E. Levine, $p$-integral harmonic sums, *Discrete Math.* **91** (1991), 249–257.
4. J. W. L. Glaisher, On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus $p^2$ or $p^3$, *Quart. J. Pure Appl. Math.* **31** (1900), 321–353.
5. J. W. L. Glaisher, On the residues of the sums of the inverse powers of numbers in arithmetic progression, *Quart. J. Pure Appl. Math.* **32** (1901), 271–305.

6. G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 4th ed., Oxford Univ. Press, London, 1960.
7. E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. Math.* **39** (1938), 350–360.
8. L. Washington, "Introduction to Cyclotomic Fields," Springer-Verlag, New York/Berlin, 1982.