Journal of Integer Sequences, Vol. 13 (2010),
Article 10.5.1

Congruences of Multiple Sums Involving Sequences Invariant Under the Binomial Transform

Sandro Mattarei
Dipartimento di Matematica
Università di Trento
via Sommarive, 14
38100 Trento, Italy
mattarei@science.unitn.it

Roberto Tauraso
Dipartimento di Matematica
Università di Roma "Tor Vergata"
via della Ricerca Scientifica
00133 Roma, Italy
tauraso@mat.uniroma2.it

Abstract

We prove several congruences modulo a power of a prime, such as

$$\sum_{0<k_1<\cdots<k_n<p} \binom{p-k_n}{3} \frac{(-1)^{k_n}}{k_1\cdots k_n} \equiv \begin{cases} -\dfrac{2^{n+1}+2}{6^{n+1}}\, p\, B_{p-n-1}(1/3) \pmod{p^2}, & \text{if } n \text{ is odd}, \\ -\dfrac{2^{n+1}+4}{n6^n}\, B_{p-n}(1/3) \pmod{p}, & \text{if } n \text{ is even}, \end{cases}$$

where n is a positive integer and p is a prime such that $p > \max(n+1, 3)$.

1 Introduction

The classical binomial inversion formula states that the linear transformation of sequences

$$T(\{a_n\}) = \left\{ \sum_{k=0}^{n} \binom{n}{k} (-1)^k a_k \right\}$$

is an involution, which means that $T \circ T$ is the identity map. Thus, T can only have two eigenvalues: 1 and -1. Denote by $\mathcal{S}_+$ and $\mathcal{S}_-$ the eigenspaces corresponding to the eigenvalue 1 and to the eigenvalue -1. These eigenspaces contain many well-known sequences, among which are

$$\{2, 1, 1, 1, \ldots\},\ \{2^{-n}\},\ \{L_n\},\ \{(-1)^n B_n\},\ \{1/(n+1)\},\ \left\{ \binom{2n}{n} 4^{-n} \right\} \in \mathcal{S}_+,$$

$$\{0, 1, 1, 1, \ldots\},\ \{2^n - (-1)^n\},\ \{F_n\},\ \left\{ (-1)^n \binom{n}{3} \right\} \in \mathcal{S}_-.$$

Here $\{F_n\}$, $\{L_n\}$, $\{B_n\}$ denote the Fibonacci, Lucas and Bernoulli numbers. For a more detailed analysis of the properties of $\mathcal{S}_+$ and $\mathcal{S}_-$ we refer the reader to the papers of Sun [3] and Wang [6]. From now on we will use the subscript k rather than the more traditional n, which takes another meaning here.

In this note we present several congruences of multiple harmonic sums with coefficients involving these invariant sequences. Our main result is the following.

Theorem 1.1. *Let n be a positive integer, and let p be a prime such that $p > n+1$. Suppose that either n is odd and $\{a_k\} \in \mathcal{S}_-$, or n is even and $\{a_k\} \in \mathcal{S}_+$. Then*

$$\sum_{0<k_1<\cdots<k_n<p} \frac{a_{p-k_n} - a_0/2}{k_1 \cdots k_n} \equiv \frac{p(n+1)}{2} \sum_{0<k_1<\cdots<k_{n+1}<p} \frac{a_{p-k_{n+1}} - a_0/2}{k_1 \cdots k_{n+1}} \pmod{p^3}.$$

The term $a_0/2$ in the congruence is immaterial when n is odd, because all sequences in $\mathcal{S}_-$ satisfy $a_0 = 0$. Note that in the extremal case $n = p-2$, whence n is odd, the congruence is actually an equality, because $a_1 = a_2$ for $\{a_k\} \in \mathcal{S}_-$ and

$$\sum_{0<k_1<\cdots<k_{p-2}<p} \frac{a_{p-k_{p-2}}}{k_1 \cdots k_{p-2}} = \frac{a_1}{(p-1)!} \sum_{0<k<p} k = \frac{p(p-1)}{2} \cdot \frac{a_1}{(p-1)!}.$$

The following result is an immediate application of Theorem 1.1 and, in case n is even, the simple fact that $\sum_{0<k_1<\cdots<k_n<p} 1/(k_1 \cdots k_n) \equiv 0 \pmod{p}$ for $p > n+1$.

Corollary 1.2. *Let n be a positive integer, and let p be a prime such that $p > n+1$. Suppose that $\{a_k\} \in \mathcal{S}_-$ if n is odd, and that $\{a_k\} \in \mathcal{S}_+$ if n is even. Then*

$$\sum_{0<k_1<\cdots<k_n<p} \frac{a_{k_1}}{k_1 \cdots k_n} \equiv - \sum_{0<k_1<\cdots<k_n<p} \frac{a_{p-k_n}}{k_1 \cdots k_n} \equiv 0 \pmod{p}.$$

The first congruence in Corollary 1.2 is obtained by applying the simultaneous substitution $k_i \mapsto p - k_{n+1-i}$ to the summation indices, and so our real contribution is the second congruence. That congruence was proved by Zhao and Sun [7] for the special case of the sequence $\{a_k\} = \left\{(-1)^k \binom{k}{3}\right\} \in \mathcal{S}_-$ and, in a different but essentially equivalent form, of the sequence $\{a_k\} = \left\{(-1)^k \left(\binom{k+1}{3} - \binom{k-1}{3}\right)\right\} \in \mathcal{S}_+$. The method used by Zhao and Sun [7] can easily be adapted to deduce the validity of Corollary 1.2 for all sequences in $\mathcal{S}_\pm$ which satisfy a second-order linear recurrence, but our proof does not need this restriction.

In Section 3 we prove a polynomial congruence, stated in Lemma 3.2, which reduces the evaluation modulo p of multiple harmonic sums (with coefficients, such as those involved in the above results) to certain single sums. We show that another polynomial congruence, which is the crucial result of Zhao and Sun [7], can be easily deduced from ours. However, our congruence is more versatile, and we exploit it in the final section together with Theorem 1.1 to prove the congruences involving Bernoulli numbers stated in the abstract, and another matching pair of congruences with the parity of n reversed. These congruences both refine (modulo p^2) and complement (covering the case where n has the opposite parity) the congruences proved by Zhao and Sun [7].

In the final Section 4, after determining all sequences in $\mathcal{S}_\pm$ which are (eventually) periodic, we use Theorem 1.1 and the tools developed in Section 3 to prove the pair of congruences stated in the abstract, and a naturally matching pair of congruences.

2 Proof of Theorem 1.1

For the reader's benefit we recall some general information on the binomial transform. Of course this can also be found in various sources, including papers of Prodinger, Sun and Wang [2, 3, 6]. If $A(x) = \sum_{k\geq 0} a_k x^k$ is the ordinary generating function of the sequence $\{a_k\}$, then it is easy to see that its binomial transform $T(\{a_k\})$ has generating sequence $\frac{1}{1-x} A\left(\frac{x}{x-1}\right)$, and so $\{a_k\} \in \mathcal{S}_\pm$ if and only if

$$\frac{1}{1-x} A\left(\frac{x}{x-1}\right) = \pm A(x). \tag{2.1}$$

After applying the substitution $x = 2y/(y-1)$ this condition takes the more symmetric form

$$\frac{1}{1-y} A\left(\frac{-2y}{1-y}\right) = \pm \frac{1}{1+y} A\left(\frac{2y}{1+y}\right).$$

The left-hand side of this equation is the generating function of an associated sequence $\{b_k\}$=$T(\{2^k a_k\})$, the binomial transform of $\{2^k a_k\}$. We conclude that $\{a_k\} \in \mathcal{S}_\pm$ occurs exactly when that generating sequence is an even or an odd function, respectively. Equivalently, $\{a_k\} \in \mathcal{S}_\pm$ occurs if and only if all odd-numbered terms b_{2k+1}, respectively all even-numbered terms b_{2k}, of the associated sequence, vanish. This statement is an equivalent formulation of a result of Sun [3, Corollary 3.3], but the above proof avoids use of exponential generating functions, which was made by Sun [3] after a suggestion of Prodinger [2].

After these preliminaries, our starting point is the following identity.

Lemma 2.1. *If $\{a_k\} \in \mathcal{S}_\pm$, then for $m, n \geq 0$ we have*

$$\sum_{k=0}^{n} \left[\binom{(m-1)n+k-1}{k} \pm (-1)^{n-k} \binom{mn}{k} \right] a_{n-k} = 0,$$

where the sign is taken accordingly.

Proof. The result can be obtained by taking $f_k = \binom{(m-1)n+k-1}{k} / \binom{n}{k}$ in the more general identity

$$\sum_{k=0}^{n} \binom{n}{k} \left[f_k \pm (-1)^{n-k} \sum_{i=0}^{k} \binom{k}{i} f_i \right] a_{n-k} = 0,$$

which holds for an arbitrary sequence $\{f_k\} \in \mathcal{S}_\pm$, with sign in accordance, and was proved by Sun [3, Theorem 4.1] by means of exponential generating functions (see also the paper of Wang [6]). To make this paper self-contained we give a direct proof. Denote by $[x^k]f(x)$ the coefficient of x^k in the Laurent series $f(x)$. Because

$$\binom{(m-1)n+k-1}{k} = [x^k] \frac{1}{(1-x)^{(m-1)n}} = [x^{-1}] \frac{1}{x^{n+1}(1-x)^{(m-1)n}} \cdot x^{n-k}$$

and

$$(-1)^{n-k} \binom{mn}{k} = [x^k] \frac{(-1)^{n-k}}{(1-x)^{mn-k+1}} = [x^{-1}] \frac{1}{x^{n+1}(1-x)^{(m-1)n+1}} \cdot \left(\frac{x}{x-1} \right)^{n-k},$$

the left-hand side of the desired identity equals

$$[x^{-1}] \frac{1}{x^{n+1}(1-x)^{(m-1)n}} \cdot \left[A(x) \pm \frac{1}{1-x} A\left(\frac{x}{x-1} \right) \right],$$

where $A(x) = \sum_{k \geq 0} a_k x^k$ is the generating function of the sequence $\{a_k\}$. The conclusion now follows from Equation (2.1). $\square$

We define the *multiple harmonic sums* of order n as

$$H_r^{(n)} = \sum_{0<k_1<k_2<\cdots<k_n \leq r} \frac{1}{k_1 k_2 \cdots k_n},$$

for $0 < n \leq r$. Interpreting the summation as ranging over the subsets of $\{1, \ldots, r\}$ of cardinality n, it is natural and convenient to extend the definition to include order zero by setting $H_r^{(0)} = 1$ for $r \geq 0$, and to stipulate that the sum vanishes unless $0 \leq n \leq r$. All congruences modulo powers of p in this paper should be read in the ring of p-adic integers, thus admitting denominators prime to p.

Proof of Theorem 1.1. Assume first that n is odd and $\{a_k\} \in \mathcal{S}_-$, where the proof is slightly simpler. Because $a_0 = 0$ and p is odd, according to Lemma 2.1 we have

$$\sum_{k=1}^{p-1} \left[\binom{(m-1)p+k-1}{k} - (-1)^k \binom{mp}{k} \right] a_{p-k} = 0.$$

By expanding the binomial coefficients for $0 < k < p$ we find

$$\binom{(m-1)p+k-1}{k} = \frac{(m-1)p}{k}\prod_{i=1}^{k-1}\left(1+\frac{(m-1)p}{i}\right) = \frac{1}{k}\sum_{j\geq 1}\big((m-1)p\big)^j H_{k-1}^{(j-1)},$$

and

$$\binom{mp}{k} = \frac{mp}{k}(-1)^{k-1}\prod_{i=1}^{k-1}\left(1-\frac{mp}{i}\right) = \frac{(-1)^k}{k}\sum_{j\geq 1}(-mp)^j H_{k-1}^{(j-1)}.$$

Consequently, the numbers $S_j = \sum_{k=1}^{p-1} H_{k-1}^{(j-1)} a_{p-k}/k$ satisfy

$$\sum_{j\geq 1}\big((m-1)^j - (-m)^j\big)\, p^j S_j = 0$$

for all nonnegative integers m. Note that $S_j = 0$ unless $1 \leq j \leq p$. Setting $f(x) = \sum_{j=1}^{p} p^j S_j (-x)^j$, the above relations show that the polynomial $f(1-x) - f(x)$ vanishes for infinitely many values of x, and hence is the zero polynomial. After a translation, it follows that $f(1/2-x) - f(1/2+x)$ is the zero polynomial. This means that the polynomial $f(1/2-x)$ is invariant under the substitution $x \mapsto -x$, hence it is an even polynomial, and so the coefficents of odd powers of x vanish. By expanding

$$f\left(1/2 - x\right) = \sum_{j\geq 1} p^j S_j \sum_{n}\binom{j}{n}(1/2)^{j-n}(-x)^n = \sum_{n}\left(\sum_{j\geq n} 2^{n-j} p^j S_j \binom{j}{n}\right)(-x)^n,$$

for each odd n we obtain the congruence

$$p^n S_n - \frac{1}{2}p^{n+1}(n+1)S_{n+1} + \frac{1}{4}p^{n+2}\binom{n+2}{2}S_{n+2} \equiv 0 \pmod{p^{n+3}}.$$

It follows, in particular, that $S_n \equiv 0 \pmod{p}$ for each odd n, and hence $S_{n+2} \equiv 0 \pmod{p}$ as well. Using this and the original congruence we conclude that $2S_n \equiv p(n+1)S_{n+1} \pmod{p^3}$, which is the desired conclusion.

Now consider the case where n is even and $\{a_k\} \in \mathcal{S}_+$. Here Lemma 2.1 yields

$$\sum_{k=1}^{p-1}\left[\binom{(m-1)p+k-1}{k} + (-1)^k\binom{mp}{k}\right] a_{p-k} = -2a_p + \frac{1}{m}\binom{mp}{p}a_0.$$

Expanding the binomial coefficients as in the first part of the proof we see that the numbers $S_j = \sum_{k=1}^{p-1} H_{k-1}^{(j-1)} a_{p-k}/k$ satisfy

$$\sum_{j\geq 1}\big((m-1)^j + (-m)^j\big)\, p^j S_j = -2a_p + \frac{1}{m}\binom{mp}{p}a_0$$

for all nonnegative integers m. Now consider the polynomial

$$g(x) = f(x) + a_p - \frac{a_0}{2}\binom{xp-1}{p-1} = \sum_{j=1}^{p} p^j S_j (-x)^j + a_p - \frac{a_0}{2}\binom{xp-1}{p-1}.$$

Note that $\binom{xp-1}{p-1} = \binom{xp}{p}/x$ is a polynomial of degree $p-1$, and is invariant under the substitution $x \mapsto 1-x$. Therefore, the relations found imply that $g(x)+g(1-x)$ vanishes for infinitely many values of x. Hence $g(x)+g(1-x)$ is the zero polynomial, and hence so is $g(1/2+x)+g(1/2-x)$. This means that the polynomial $g(x+1/2)$ is an odd polynomial, and so the coefficents of even powers of x vanish. Arguing as in the proof of part (i), for each even $n>0$ we obtain the congruence

$$p^n S_n - \frac{1}{2}p^{n+1}(n+1)S_{n+1} + \frac{1}{4}p^{n+2}\binom{n+2}{2}S_{n+2} \equiv [x^n]\,\frac{a_0}{2}\binom{(x+1/2)p-1}{p-1} \pmod{p^{n+3}}.$$

Because the right-hand side of this congruence depends only on the initial term a_0 of our sequence, we can compute it by considering the special sequence $a_k = (a_0/2)\cdot\{2,1,1,1,\ldots\} \in \mathcal{S}_+$. In this case we have $S_n = (a_0/2)H_{p-1}^{(n)}$, which is easily seen to vanish modulo p as soon as $p > n+1$, for example by setting $x=1$ in Lemma 3.2 of the next section. We conclude that

$$S_n - \frac{1}{2}p(n+1)S_{n+1} \equiv \frac{a_0}{2}H_{p-1}^{(n)} - \frac{a_0}{4}p(n+1)H_{p-1}^{(n+1)} \pmod{p^3},$$

for an arbitrary sequence $\{a_k\} \in \mathcal{S}_+$. □

3 Some polynomial congruences

The main result of this section is Lemma 3.2, which shows that certain sums involving higher order harmonic numbers are equivalent modulo p to other sums which are easier to handle. We first need a preliminary result.

Lemma 3.1. *For a positive integer m, the identity*

$$\sum_{0\le k<m}\binom{y}{k}(-x)^k = 1 + \sum_{n>0}(-y)^n \sum_{0<k<m} H_{k-1}^{(n-1)}\frac{x^k}{k}$$

holds in the polynomial ring $\mathbb{Q}[x,y]$ in two indeterminates.

Proof. For $k>0$, by expanding

$$\binom{y}{k} = \frac{y}{k}\binom{y-1}{k-1} = \frac{(-1)^{k-1}y}{k}\prod_{0<i<k}\left(1-\frac{y}{i}\right)$$

we see that the coefficient of y^n in the polynomial without constant term $\binom{y}{k}$ equals

$$\frac{(-1)^{k+n}}{k}\sum_{0<i_1<\cdots<i_{n-1}<k}\frac{1}{i_1\cdots i_{n-1}} = \frac{(-1)^{k+n}}{k}H_{k-1}^{(n-1)},$$

properly interpreted to equal $(-1)^{k-1}/k$ when $n=1$ (because the sum has a unique term, which is an empty product), and to vanish when $n>k$ (because the sum is empty). The desired conclusion follows. □

Lemma 3.2. *Let n be a positive integer and let p be a prime with $p > n+1$. Then we have the polynomial congruence*

$$\sum_{k=1}^{p-1} H_{k-1}^{(n-1)} \frac{x^k}{k} \equiv (-1)^{n-1} \sum_{k=1}^{p-1} \frac{(1-x)^k}{k^n} \pmod{p}. \tag{3.1}$$

The case $n = 1$ of Lemma 3.2 is well known and due to the fact that in this case the left-hand side is congruent modulo p to the polynomial $\bigl(1 - x^p - (1-x)^p\bigr)/p$, which is invariant under the substitution $x \mapsto 1-x$. The general case can be proved by induction starting from this special case or, more directly and perhaps more insightfully, as follows.

Proof. The left-hand side of the identity of Lemma 3.1 may be viewed as a polynomial in the indeterminate y over the field of rational functions $\mathbb{Q}(x)$ (the field of quotients of $\mathbb{Q}[x]$). Because of the binomial expansion, it takes the same values as the function $y \mapsto (1-x)^y$ when evaluated for $y = 0, \dots, m-1$. Furthermore, having degree less than m it is completely determined by those values, for example through Lagrange's interpolation formula.

Over a field E of characteristic p, and with $m = p$, Lagrange's interpolation formula takes a particularly nice shape: for any polynomial $f(y) \in E[y]$ of degree less than p we have

$$f(y) = f(0)(1 - y^{p-1}) - \sum_{n=1}^{p-1} y^n \sum_{k \in \mathbb{F}_p^*} f(k) k^{-n}.$$

In this special case the use of Lagrange's interpolation formula can be replaced by direct verification: geometric summation shows that the polynomial $\sum_{n=1}^{p-1} (y/k)^n$ takes the value -1 for $y = k$, and vanishes on the remaining elements of $\mathbb{F}_p$.

By taking as f the left-hand side of the identity of Lemma 3.1, with $m = p$, viewed over the field $E = \mathbb{F}_p(x)$, we obtain

$$\sum_{k=0}^{p-1} \binom{y}{k} (-x)^k = 1 - y^{p-1} - \sum_{n=1}^{p-1} y^n \sum_{k=1}^{p-1} (1-x)^k / k^n$$

in the polynomial ring $E[y]$. The conclusion now follows from Lemma 3.1 by equating the coefficient of y^n in both sides of this identity, and rewriting the result as a congruence modulo p in the polynomial ring $\bigl(\mathbb{Q}(x)\bigr)[y]$. $\square$

The polynomial at the right-hand side of congruence (3.1) has some obvious roots in the prime field $\mathbb{F}_p$ for all primes $p > n+1$, namely, 0 and 1, and also 2 when n is even. This last fact occurs because the value modulo p of that polynomial at $x = 2$ is multiplied by $(-1)^{n-1}$ when replacing the summation variable k with $p - k$. By evaluating congruence (3.1) on $x = 1$ we recover the basic fact that $H_{p-1}^{(n)} \equiv 0 \pmod{p}$ for $0 < n < p-1$. Evaluation for $x = 2$ yields

$$\sum_{0 < k_1 < \cdots < k_n < p} \frac{2^{k_n}}{k_1 \cdots k_n} \equiv 0 \pmod{p} \tag{3.2}$$

for even n with $0 < n < p-1$. Equation (1.1) of Sun [5], which reads $\sum_{0<k<p} H_k/(k2^k) \equiv 0 \pmod{p}$, follows from the special case $n = 2$ of our Equation (3.2) via the simple manipulation

$$\sum_{0<j\leq k<p} \frac{1}{jk2^k} = \sum_{0<j<p} \frac{1}{j} \sum_{0<k<p} \frac{1}{k2^k} - \sum_{0<k<j<p} \frac{1}{jk2^k} \equiv \sum_{0<j<k<p} \frac{1}{(p-j)(p-k)2^{p-k}} \pmod{p}.$$

We can use Lemma 3.2 to give a direct, rather than inductive proof, of the following crucial result of Zhao and Sun [7, Theorem 1.2].

Corollary 3.3 (Zhao and Sun [7]). *Let n be a positive integer and let p be a prime with $p > n+1$. Then we have the polynomial congruence*

$$\sum_{0<k_1<\cdots<k_n<p} \frac{(1-x)^{k_1}}{k_1\cdots k_n} \equiv (-1)^{n-1} \sum_{0<k_1<\cdots<k_n<p} \frac{x^{k_1}}{k_1\cdots k_n} \pmod{p}.$$

Proof. After applying the simultaneous substitution $k_i \mapsto p - k_{n+1-i}$ to the summation variables, we invoke Lemma 3.2 with x^{-1} in place of x and obtain

$$\begin{aligned}
\sum_{0<k_1<\cdots<k_n<p} \frac{x^{k_1}}{k_1\cdots k_n} &= \sum_{0<k_1<\cdots<k_n<p} \frac{x^{p-k_n}}{(p-k_1)\cdots(p-k_n)} \\
&\equiv (-1)^n x^p \sum_{0<k_1<\cdots<k_n<p} \frac{x^{-k_n}}{k_1\cdots k_n} \\
&\equiv -x^p \sum_{k=1}^{p-1} \frac{(1-x^{-1})^k}{k^n} \\
&\equiv -\sum_{k=1}^{p-1} \frac{(x-1)^k x^{p-k}}{k^n} \pmod{p}.
\end{aligned}$$

If we apply the substitution $x \mapsto 1-x$ to this last polynomial we obtain

$$\sum_{k=1}^{p-1} \frac{x^k(x-1)^{p-k}}{k^n} = \sum_{k=1}^{p-1} \frac{x^{p-k}(x-1)^k}{(p-k)^n} \equiv (-1)^n \sum_{k=1}^{p-1} \frac{(x-1)^k x^{p-k}}{k^n} \pmod{p},$$

which equals $(-1)^{n-1}$ times the original polynomial. □

4 Sums with periodic coefficient sequences

In this final section we prove the pair of congruences stated in the abstract, and a naturally matching pair of congruences. They concern multiple sums such as those in Theorem 1.1 and Corollary 1.2, for special sequences $\{a_k\}$ of coefficients, which are periodic of period six. The special significance of those sequences lies in the fact that, up to addition of multiples of the nearly constant sequences $\{(1 \pm 1), 1, 1, 1, \ldots\} \in \mathcal{S}_\pm$, they are the only (eventually) periodic sequences in $\mathcal{S}_{\pm}$. To prove this fact we start with some more general considerations on sequences in $\mathcal{S}_{\pm}$ with a rational generating function.

Several sequences $\{a_k\} \in \mathcal{S}_{\pm}$ of interest satisfy a linear recurrence. It is well known that a sequence $\{a_k\}$ satisfies a linear recurrence exactly when its generating function $A(x) = \sum_{k\geq 0} a_k x^k$ is a rational function. If $\{a_k\}$ is any sequence with rational generating function $A(x)$, then the generating function $\frac{1}{1-x} A\left(\frac{x}{x-1}\right)$ of its binomial transform $T(\{a_k\})$ has a zero of multiplicity s (or a pole of multiplicity $-s$ when s is negative) at $\xi \in \mathbb{C} \setminus \{1\}$ if and only if $A(x)$ has a zero of the same multiplicity s at $\xi/(\xi-1) = (1-\xi^{-1})^{-1}$. The case $\xi = 1$ is special, because the generating function of $T(\{a_k\})$ has a zero of multiplicity s at 1 if and only if $A(x)$ has a zero of multiplicity $s+1$ at ∞. Recall that the multiplicity of ∞ as a zero of a rational function is the difference of the degrees of its denominator and numerator. Because of Equation (2.1), it follows that if $\{a_k\} \in \mathcal{S}_{\pm}$ satisfies a linear recurrence, then the multiplicity of $\xi \in \mathbb{C} \setminus \{1\}$ as a zero of its generating function $A(x)$ equals the multiplicity of $(1-\xi^{-1})^{-1}$, and the multiplicity of 1 is one less than the multiplicity of ∞.

Now consider a sequence $\{a_k\} \in \mathcal{S}_{\pm}$ which is eventually periodic, which means that it satisfies, from some point on, a linear recurrence $a_{k+d} = a_k$ for some positive integer d. Then its generating function $A(x)$ has the form $f(x)/(1-x^d)$, where $f(x)$ is a polynomial, which has degree less than d exactly when the sequence is periodic from the start. Hence $A(x)$ has only simple poles, and at complex roots of unity. However, the only roots of unity ξ such that $\xi/(\xi-1)$ is also a root of unity are the two primitive sixth roots of unity, which are the roots of the polynomial $1-x+x^2$. The discussion in the previous paragraph shows that the poles of $A(x)$ can only occur at 1 and at the primitive sixth roots of unity. In particular, the sequence $\{a_k\}$ can only have period 1 or 6. That discussion also shows that $f(x)$ has degree at most d, with equality if and only if 1 is a pole of $A(x)$. In terms of the sequence $\{a_k\}$, this means that if it is eventually periodic then either it is periodic from the start, or from its second term a_1. In connection with our work, note that the first term a_0 of the sequence enters our Theorem 1.1 only in one case, and is immaterial in Corollary 1.2.

We can now determine all sequences $\{a_k\} \in \mathcal{S}_{\pm}$ which are eventually periodic. In fact, if such a sequence is not periodic from the start, it becomes so after adding to it a suitable multiple of the sequence $\{(1 \pm 1), 1, 1, 1, \ldots\} \in \mathcal{S}_{\pm}$, with the effect of removing the pole at 1 from its generating function $A(x)$. Therefore, it suffices to consider a fully periodic sequence $\{a_k\}$. Because the only poles of $A(x)$ are simple, and at the primitive sixth roots of unity, we have $A(x) = \big((a_1 - a_0)x + a_0\big)/(1-x+x^2)$. Hence $\{a_k\}$ has period exactly six, and a simple calculation shows that $A(x)$ is a scalar multiple of

$$\frac{-x}{1-x+x^2} = \sum_{k=0}^{\infty} (-1)^k \binom{k}{3} x^k = -x - x^2 + x^4 + x^5 + \cdots$$

or

$$\frac{2-x}{1-x+x^2} = \sum_{k=0}^{\infty} (-1)^k \left(\binom{k+1}{3} - \binom{k-1}{3} \right) x^k = 2 + x - x^2 - 2x^3 - x^4 + x^5 + \cdots ,$$

according as $\{a_k\}$ belongs to $\mathcal{S}_-$ or $\mathcal{S}_+$.

Now that we have shown the special significance of these sequences, we proceed to prove the pair of congruences stated in the abstract, and a matching pair of congruences.

Theorem 4.1. *Let n be a positive integer and let p be a prime with $p > \max(n+1, 3)$. Consider the sequence in $\mathcal{S}_-$ given by $u_k = (-1)^k\left(\frac{k}{3}\right)$, and the sequence in $\mathcal{S}_+$ given by $v_k = (-1)^k\left(\left(\frac{k+1}{3}\right) - \left(\frac{k-1}{3}\right)\right)$. Let $B_m(x)$ denote the Bernoulli polynomials. Then*

$$\sum_{0<k_1<\cdots<k_n<p} \frac{u_{p-k_n}}{k_1\cdots k_n} \equiv \begin{cases} \dfrac{2^n+1}{3\cdot 6^n}\, p\, B_{p-n-1}(1/3) \pmod{p^2}, & \text{if } n \text{ is odd,} \\ \dfrac{2^{n+1}+4}{n6^n}\, B_{p-n}(1/3) \pmod{p}, & \text{if } n \text{ is even,} \end{cases}$$

and

$$\sum_{0<k_1<\cdots<k_n<p} \frac{v_{p-k_n}}{k_1\cdots k_n} \equiv \begin{cases} \left(\dfrac{(2^n-1)(3^n-1)}{2\cdot 6^n} - \dfrac{1}{n+1}\right) p\, B_{p-n-1} \pmod{p^2}, & \text{if } n \text{ is even,} \\ \dfrac{(2^{n-1}-1)(3^{n-1}-1)}{n6^{n-1}}\, B_{p-n} \pmod{p}, & \text{if } n \text{ is odd.} \end{cases}$$

Proof. We first prove the former pair of congruences, starting with the case where n is even. Let ω be a complex primitive cubic root of unity, and note that $\left(\frac{k}{3}\right) = (\omega^k - \omega^{-k})/(\omega - \omega^{-1})$ for all k. Interpreting congruences modulo p in the ring $\mathbb{Z}[\omega]$ of Eisenstein integers, Lemma 3.2 yields

$$\begin{aligned} \sum_{k=1}^{p-1} H_{k-1}^{(n-1)} \frac{u_{p-k}}{k} &= \frac{1}{\omega - \omega^{-1}} \left((-\omega)^p \sum_{k=1}^{p-1} H_{k-1}^{(n-1)} \frac{(-\omega)^{-k}}{k} - (-\omega)^{-p} \sum_{k=1}^{p-1} H_{k-1}^{(n-1)} \frac{(-\omega)^{k}}{k} \right) \\ &\equiv \frac{(-1)^{n-1}}{\omega - \omega^{-1}} \left((-\omega)^p \sum_{k=1}^{p-1} \frac{(-\omega)^{k}}{k^n} - (-\omega)^{-p} \sum_{k=1}^{p-1} \frac{(-\omega)^{-k}}{k^n} \right) \pmod{p} \\ &= -\sum_{k=1}^{p-1} \frac{u_{p+k}}{k^n}, \end{aligned}$$

where we have used the fact that $1 - (-\omega)^{-1} = -\omega$, in the second passage. The coefficient $-u_{p+k}$ of $1/k^n$ in the last formula takes the values $0, 1, 1, 0, -1, -1$ according as $p + k \equiv 0, 1, 2, 3, 4, 5 \pmod 6$. According to Sun [4, Lemma 2.1] combined with Fermat's little theorem we have

$$\sum_{\substack{0<k<p \\ k\equiv r \pmod 6}} \frac{1}{k^n} \equiv \frac{1}{n6^n} \left(B_{p-n}\left(\left\{\frac{r}{6}\right\}\right) - B_{p-n}\left(\left\{\frac{r-p}{6}\right\}\right)\right) \pmod{p},$$

for any integer r, under our hypothesis that $p > \max(n+1, 3)$. Here $\{t\} = t - [t]$ denotes the fractional part of the real number t. All the values of the Bernoulli polynomials involved in this formula can be obtained from just one of them, using the fact that the Bernoulli polynomials satisfy the reflection property and the multiplication formula

$$B_m(1-x) = (-1)^m B_m(x), \quad \text{and} \quad B_m(ax) = a^{m-1} \sum_{k=0}^{a-1} B_m(x + k/a),$$

for $m, a > 0$, see Ireland and Rosen [1, p. 248]. Thus, taking into account that $p-n$ is odd we find

$$B_{p-n}(0) = B_{p-n}(1/2) = 0, \qquad B_{p-n}(2/3) = -B_{p-n}(1/3),$$
$$B_{p-n}(1/6) = -B_{p-n}(5/6) = \left(2^{n-(p-1)}+1\right) B_{p-n}(1/3).$$

Carrying out separate calculations according as $p \equiv \pm 1 \pmod 6$, in both cases we obtain

$$-\sum_{k=1}^{p-1} \frac{u_{p-k}}{k^n} \equiv \frac{2^{n+1}+4}{n6^n} B_{p-n}(1/3) \pmod p,$$

which proves the case of our first pair of congruences where n is even. When n is odd, the congruence which we have just proved holds with $n+1$ in place of n. Combining this with Theorem 1.1 we obtain

$$\begin{aligned}\sum_{k=1}^{p-1} H_{k-1}^{(n-1)} \frac{u_{p-k}}{k} &\equiv \frac{p(n+1)}{2} \sum_{k=1}^{p-1} H_{k-1}^{(n)} \frac{u_{p-k}}{k} \pmod{p^3} \\ &\equiv \frac{2^{n+1}+2}{6^{n+1}} pB_{p-n-1}(1/3) \pmod{p^2},\end{aligned}$$

which proves the other case of the first pair of congruences.

We deal with the second pair of congruences in an entirely similar manner, using the fact that $\left(\frac{k+1}{3}\right) - \left(\frac{k-1}{3}\right) = \omega^k + \omega^{-k}$ for all k. Here $-v_{p+k}$ takes the values $-2, -1, 1, 2, 1, -1$ according as $p+k \equiv 0, 1, 2, 3, 4, 5 \pmod 6$. When n is odd, whence $p-n$ is even, the values of the Bernoulli polynomial $B_{p-n}(x)$ involved are

$$B_{p-n}(1/2) = \left(2^{n-(p-1)}-1\right) B_{p-n}, \qquad B_{p-n}(1/3) = B_{p-n}(2/3) = \frac{3^{n-(p-1)}-1}{2} B_{p-n},$$
$$B_{p-n}(1/6) = B_{p-n}(5/6) = \frac{6^{n-(p-1)}-3^{n-(p-1)}-2^{n-(p-1)}+1}{2} B_{p-n},$$

all expressed in terms of the Bernoulli numbers $B_n = B_n(0)$. Thus, when n is odd we find

$$\sum_{k=1}^{p-1} H_{k-1}^{(n-1)} \frac{v_{p-k}}{k} \equiv -\sum_{k=1}^{p-1} \frac{v_{p+k}}{k^n} \equiv \frac{(2^{n-1}-1)(3^{n-1}-1)}{n6^{n-1}} B_{p-n} \pmod p.$$

When n is even, this congruence holds with $n+1$ in place of n. According to Zhou and Cai [8, Remark at p. 1332], for $p > j+2$ we have

$$H_{p-1}^{(j)} \equiv \begin{cases} 0 \pmod{p^2}, & \text{if } j \text{ is odd}, \\ -\dfrac{p}{j+1} B_{p-j-1} \pmod{p^2}, & \text{if } j \text{ is even}. \end{cases}$$

In combination with Theorem 1.1, noting that $v_0 = 2$, this yields

$$\begin{aligned}\sum_{k=1}^{p-1} H_{k-1}^{(n-1)} \frac{v_{p-k}}{k} &\equiv \frac{p(n+1)}{2} \sum_{k=1}^{p-1} H_{k-1}^{(n)} \frac{v_{p-k}}{k} + H_{p-1}^{(n)} - \frac{p(n+1)}{2} H_{p-1}^{(n+1)} \pmod{p^3} \\ &\equiv \frac{p}{2} \frac{(2^n-1)(3^n-1)}{6^n} B_{p-n-1} - \frac{p}{n+1} B_{p-n-1} \pmod{p^2},\end{aligned}$$

as desired. $\square$

References

[1] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990.

[2] H. Prodinger, Some information about the binomial transform, *Fibonacci Quart.* **32** (1994), 412–415.

[3] Z. H. Sun, Invariant sequences under binomial transformation, *Fibonacci Quart.* **39** (2001), 324–333.

[4] Z. H. Sun, Congruences involving Bernoulli polynomials, *Discrete Math.* **308** (2008), 71–112.

[5] Z. W. Sun, Arithmetic of harmonic numbers, preprint arXiv:math.NT/0911.4433v4.

[6] Y. Wang, Self-inverse sequences related to a binomial inverse pair, *Fibonacci Quart.* **43** (2005), 46–52.

[7] L. L. Zhao, Z. W. Sun, Some curious congruences modulo primes, *J. Number Theory* **130** (2010), 930–935.

[8] X. Zhou and T. Cai, A generalization of a curious congruence on harmonic sums, *Proc. Amer. Math. Soc.* **135** (2007), 1329–1333.

2000 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B65, 05A10, 05A19.
Keywords: binomial transform, multiple sum, congruence, Bernoulli polynomial.

Received November 5 2009; revised version received April 16 2010. Published in *Journal of Integer Sequences*, April 16 2010.

Return to Journal of Integer Sequences home page.