CONGRUENCES FOR VALUES OF SYMMETRIC POLYNOMIALS MODULO LARGE POWERS OF A PRIME

JULIAN ROSEN

Abstract. Harmonic numbers, which are partial sums of the harmonic series, and various generalizations of the harmonic numbers are known to satisfy many congruences. The present work considers congruences of a particular shape, involving values of symmetric functions generalizing the harmonic numbers. The congruences we consider can hold modulo arbitrarily large powers of a prime. We give a conditional classification of all congruences of the shape we consider.

1. Introduction

Wolstenholme’s congruence, proved in 1862, is the result that the numerator of the harmonic number

\[ H_{p-1} := 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \]

is divisible by \( p^2 \) for every prime \( p \geq 5 \). The harmonic number above can be viewed as the value of first elementary symmetric polynomial in \( p-1 \) variables

\[ e_1 = e_1(x_1, \ldots, x_{p-1}) := x_1 + \ldots + x_{p-1} \in \mathbb{Q}[x_1, \ldots, x_{p-1}] \]

evaluated at \( x_i = i^{-1} \). More generally the value of the \( n \)-th elementary symmetric function

\[ e_n := \sum_{i_1 < \ldots < i_n} x_{i_1} \ldots x_{i_n} \]

evaluated at \( x_i = i^{-1} \) (\( i = 1, 2, \ldots, p-1 \)) has numerator divisible by \( p^2 \) or \( p \) when \( n \) is odd or even respectively (for \( p \) is sufficiently large). Similar results are known for the power sum symmetric functions (these and many other related congruences can be found in [6]). In the present work we investigate similar congruences for arbitrary symmetric functions. We give an example here.

There are known extensions of the congruences above in terms of Bernoulli numbers:

\[ e_n \left( \frac{1}{1}, \ldots, \frac{1}{p-1} \right) \equiv \begin{cases} \frac{-n(n+1)}{2(n+2)} p^2 B_{p-n-2} \pmod{p^3}, & n \text{ odd}, \\ \frac{1}{n+1} p B_{p-n-1} \pmod{p^2}, & n \text{ even}, \end{cases} \]

These expressions lead to the congruence, for any integer \( n \geq 1 \),

\[ 2e_{2n-1} \left( \frac{1}{1}, \ldots, \frac{1}{p-1} \right) - 2n e_{2n} \left( \frac{1}{1}, \ldots, \frac{1}{p-1} \right) \pmod{p^3} \]
for $p$ sufficiently large, which involves two different symmetric functions. To account for the factor of $p$ in the second term, it is convenient to include an explicit factor of $p^k$ with each term $e_k$, or equivalently to evaluate our symmetric functions at $x_i = p^{i-1}$ (for $i = 1, 2, \ldots, p - 1$). In this way we can express (2) as the congruence

$$2 e_{2n-1} \left( \frac{p}{1}, \ldots, \frac{p}{p-1} \right) - 2n e_{2n} \left( \frac{p}{1}, \ldots, \frac{p}{p-1} \right) \equiv 0 \mod p^{2n+2},$$

again for $p$ sufficiently large. We consider congruences like (3), with the expression $2 e_{2n-1} - 2n e_{2n}$ replaced by an arbitrary symmetric function.

**Question 1.** For each positive integer $n$, determine the set of symmetric functions $f$ for which the congruence

$$(\star) \quad f \left( \frac{p}{1}, \frac{p}{2}, \ldots, \frac{p}{p-1} \right) \equiv 0 \mod p^n$$

holds for all primes $p$ sufficiently large.

In the present work we give a conditional solution to Question 1. We produce for each $n$ an explicit collection of symmetric functions $f$ for which the congruence $(\star)$ holds. We show that it would follow from a conjecture on the modulo $p$ independence of Bernoulli numbers that our collection actually contains all $f$ for which $(\star)$ holds.

We construct our symmetric functions from certain formal infinite series identities. An example of such an identity is

$$\sum_{k=1}^{\infty} (-1)^k e_k \left( \frac{p}{1}, \ldots, \frac{p}{p-1} \right) = 0,$$

which holds for $p \geq 3$ (note that for any fixed $p$ the sum is finite). Reducing mod $p^n$ shows that the symmetric function

$$f = \sum_{k=1}^{n-1} (-1)^k e_k$$

satisfies $(\star)$. We find a family of series identities, of which (4) is the first, and we use these identities to construct our collection of symmetric functions for which $(\star)$ holds.

1.1. **Recent related results.** Tauraso [5] showed that $(\star)$ holds for $n = 6$, with $f = e_1 - e_2 + \frac{1}{6} p_3$, where $p_3$ is a power sum symmetric function. Several other similar results are also given in [5].

Mestrovic [1] recently gave a congruence for the binomial coefficient $\binom{2p-1}{p-1}$ modulo $p^7$ involving multiple harmonic sums. The proof utilizes a number of congruences of the form $(\star)$. Variations on this congruence are given in [2], Sec. 2. Generalizations of Mestrovic’s congruence, holding modulo arbitrarily large powers of $p$, were given by the author in [4].

\footnote{In fact this congruence holds modulo $p^{2n+3}$}
1.2. **Multiple harmonic sums.** Recall that a composition is a finite ordered list of positive integers. The *weight* of a composition \( s = (s_1, \ldots, s_k) \) is \( w(s) := s_1 + \ldots + s_k \). For \( s \) a composition and \( n \) a positive integer, the *multiple harmonic sum* is defined by

\[
H_n(s) := \sum_{n \geq n_1 > \ldots > n_k \geq 1} \frac{1}{n_1^{s_1} \ldots n_k^{s_k}} \in \mathbb{Q}.
\]

We state an equivalent form of Question 1 in terms of multiple harmonic sums:

**Question 1a.** For each positive integer \( n \), determine the set of congruences

\[
\sum_{w(s)<n} \alpha_s p^{w(s)} H_{p-1}(s) \equiv 0 \mod p^n
\]

holding for \( p \) sufficiently large, where the coefficients \( \alpha_s \) are rational and satisfy \( \alpha_s = \alpha_{s'} \) whenever the composition \( s' \) is obtained from \( s \) by rearranging the elements.

In a recent work [3], we consider a more general version of Question 1a with the hypothesis \( \alpha_s = \alpha_{s'} \) omitted. This is equivalent to a version of Question 1 with symmetric functions replaced by quasi-symmetric functions.

2. **Algebraic setup**

Recall that a *symmetric function* over \( \mathbb{Q} \) is a formal power series of bounded degree in countably many variables, with coefficients in \( \mathbb{Q} \), that is invariant under any permutation of the variables. Given a finite unordered list of elements of \( \mathbb{Q} \) (or more generally, of elements of any \( \mathbb{Q} \)-algebra), it makes sense to evaluate a symmetric function at these elements. The set of symmetric functions over \( \mathbb{Q} \) is a commutative ring, which we denote \( \Lambda_{\mathbb{Q}} \) or simply \( \Lambda \). The fundamental theorem of symmetric functions says that the elementary symmetric functions freely generate \( \Lambda \) as a \( \mathbb{Q} \)-algebra.

For every prime \( p \) there is a ring homomorphism

\[
\varphi_p : \Lambda \rightarrow \mathbb{Q},
\]

\[
f \mapsto f \left( \frac{p}{1}, \ldots, \frac{p}{p-1} \right).
\]

Following a notation used in the study of finite multiple zeta values, for \( n \geq 1 \) we set

\[
A_n := \prod_p \mathbb{Z}/(p^n) \oplus \mathbb{Z}/(p^n).
\]

An element of \( A_n \) is a class \( a_p \in \mathbb{Z}/(p^n) \) for almost all \( p \), and two families of classes \( a_p, a'_p \) determine the same element of \( A_n \) if and only if \( a_p \equiv a'_p \mod p^n \) almost all \( p \). For any \( f \in \Lambda \) and any prime \( p \) not dividing the denominator of any coefficient in \( f \), we have \( \varphi_p(f) \in \mathbb{Z}(p) \). Reducing these elements modulo \( p^n \) gives a ring homomorphism

\[
\varphi^{[n]} : \Lambda \rightarrow A_n
\]

\[
f \mapsto (\varphi_p(f) \mod p^n).
\]

The following is an equivalent form of Question 1, stated in terms of \( \varphi^{[n]} \):

**Question 1b.** For each positive integer \( n \), describe \( \ker \varphi^{[n]} \).
The congruence (1) implies that \( \varphi_p^{[n+1]}(e_n) = 0 \) for all \( n \geq 1 \) (in fact it is true that \( \varphi_p^{[n+2]}(e_n) = 0 \) when \( n \) is odd, but we will not need this fact). Motivated by this we define a grading on \( \Lambda \), which we call the grading by \( H \)-degree, by taking \( e_n \) to be homogeneous of \( H \)-degree \( n + 1 \) and extending multiplicatively (this determines the grading because \( \Lambda \) is a free algebra on the \( e_n \)). For example the element \( e_1 e_2 - 2e_4 \) is homogeneous of \( H \)-degree 5.

Take \( f \in \Lambda \) and let

\[
\sum_n f_n
\]

with \( f_n \) homogeneous of \( H \)-degree \( n \). We define

\[
v(f) := \inf \{ n : f_n \neq 0 \} \in \mathbb{Z}_{\geq 0} \cup \{ \infty \}.
\]

We also define for each \( n \) an ideal

\[
\mathcal{I}_n := \{ f \in \Lambda : v(f) \geq n \}.
\]

It follows from the congruences (1) that \( \mathcal{I}_n \subset \text{Ker} \varphi^{[n]} \), and we will denote by \( \tilde{\varphi}^{[n]} \) the induced map

\[
\tilde{\varphi}^{[n]} : \Lambda / \mathcal{I}_n \to A_n.
\]

To answer Question 1 it suffices to determine \( \ker \tilde{\varphi}^{[n]} \). A convenient system of coset representatives of \( \mathcal{I}_n \) in \( \Lambda \) is given by the symmetric functions of \( H \)-degree less than \( n \).

3. A Family of Congruences

For \( p \) an odd prime, consider the polynomial

\[
f_p(t) := \binom{pt - 1}{p - 1} = \frac{(pt - 1)(pt - 2) \ldots (pt - (p-1))}{(p-1)!} \in \mathbb{Q}[t],
\]

which is seen to satisfy the functional equation \( f_p(t) = f_p(1-t) \). We can express \( f_p(t) \) in the form

\[
f_p(t) = \left(1 - \frac{p}{1} t\right) \left(1 - \frac{p}{2} t\right) \ldots \left(1 - \frac{p}{p-1} t\right)
= \sum_{k \geq 0} (-1)^k e_k \left(\frac{p}{1}, \ldots, \frac{p}{p-1}\right) t^k.
\]

Using this expression and computing the coefficient of \( t^n \) in the functional equation proves:

**Proposition 3.1.** For all \( k \geq 0 \) and all primes \( p \geq 3 \),

\[
e_k \left(\frac{p}{1}, \ldots, \frac{p}{p-1}\right) + \sum_{j \geq k} (-1)^{j+1} \binom{j}{k} e_j \left(\frac{p}{1}, \ldots, \frac{p}{p-1}\right) = 0.
\]

Note that the sum appearing above is finite, as terms vanish whenever \( j \geq p \). We use Proposition 3.1 to generate symmetric functions satisfying congruences.
Definition 3.2. For \( n, k \geq 0 \), define
\[
\beta^{[n]}_k := e_k + \sum_{j \geq k} (-1)^{j+1} \binom{j}{k} e_j \in \Lambda / \mathcal{I}_n.
\]
This sum is finite, as \( e_j \in \mathcal{I}_n \) once \( j \) is sufficiently large.

For \( n \geq 0 \), define an ideal
\[
I^{[n]} := (\beta^{[n]}_0, \beta^{[n]}_1, \ldots) \subset \Lambda / \mathcal{I}_n.
\]
We have \( \beta^{[n]}_k = 0 \) whenever \( k \geq n - 1 \) (or \( k \geq n - 2 \) and \( k \) is even). Proposition 3.1 implies
\[
\beta^{[n]}_k \in \ker \tilde{\varphi}^{[n]}
\]
for all \( k \) and \( n \). We can now describe our family of congruences.

Theorem 3.3. Let \( n \) be a non-negative integer and suppose \( f \in \Lambda \) satisfies \( \overline{f} \in I^{[n]} \), where \( \overline{f} \) is the reduction of \( f \) modulo \( \mathcal{I}_n \). Then the congruence
\[
f \left( \frac{p}{1}, \ldots, \frac{p}{p-1} \right) \equiv 0 \mod p^n
\]
holds for all \( p \) sufficiently large.

Proof. This is equivalent to the inclusion \( I^{[n]} \subset \ker \tilde{\varphi}^{[n]} \), which follows from Proposition 3.1. \( \square \)

4. Mod \( p \) structure of Bernoulli numbers

In this section we discuss a conjecture of Zhao regarding the structure of the Bernoulli numbers modulo \( p \). We begin with an example. Wolsenholme’s congruence implies that \( e_1 \in \ker \varphi^{[3]} \). To determine whether \( e_1 \in \ker \varphi^{[4]} \), we need to know whether the congruence
\[
e_1 \left( \frac{p}{1}, \ldots, \frac{p}{p-1} \right) \equiv 0 \mod p^4
\]
holds for all sufficiently large \( p \) (we know this holds modulo \( p^3 \) for \( p \geq 5 \)). Using Eq. (1) this is equivalent to asking whether the numerator of the Bernoulli number \( B_{p-3} \) is divisible by \( p \) for all sufficiently large \( p \). It is certainly believed that this should not hold: this would contradict, for example, the conjecture that there are infinitely many regular primes. At present, however, this is not known.

Primes for which \( p | B_{p-3} \) are known as Wolstenholme primes and only two are known: 16,843 and 2,124,679. A simple heuristic suggests that there should be infinitely many Wolstenholme primes, and that the number smaller than \( x \) should grow like \( \log \log x \).

The conjecture that \( p \nmid B_{p-3} \) for infinitely many \( p \) (which is equivalent (6) failing for infinitely many \( p \)) has a generalization due to Zhao ([7], Conjecture 2.1). We state a form of this conjecture here.
Conjecture 4.1. Let $n$ be a positive integer, and suppose $h \in \mathbb{Q}[x_3, x_5, \ldots, x_{2n+1}]$ is non-zero and homogeneous (where $\deg(x_{2k+1}) = 2k + 1$). Then there exist infinitely many primes $p$ such that $p$ does not divide the numerator of $h(B_{p-3}, B_{p-5}, \ldots, B_{p-2n-1})$.

5. A conditional converse to Theorem 3.3

The truth of Conjecture 4.1 would allow us to make Theorem 3.3 biconditional:

Theorem 5.1. Assume the truth of Conjecture 4.1. Suppose $f \in \Lambda$ and $n$ is a positive integer, and let $I_n$ be given by Definition 3.2. Then the congruence

$$f \left( \frac{p}{1}, \ldots, \frac{p}{p-1} \right) \equiv 0 \mod p^n$$

holds for all $p$ sufficiently large if and only if $\overline{f} \in I_n$, where $\overline{f}$ is the reduction of $f$ modulo $I_n$.

Proof. This is the statement that $I_n = \ker \varphi[n]$. Theorem 3.3 implies $I_n \subset \ker \varphi[n]$, so we need to show $I_n \supset \ker \varphi[n]$.

Take $f \in \ker \varphi[n]$. We have

$$\beta_{2k+1} = 2e_{2k+1} + \sum_{j \geq 2k+2} (-1)^{j+1} \left( \frac{j}{2k+1} \right) e_j.$$

we we can find an element $g \in \mathbb{Q}[e_2, e_4, \ldots] \subset \Lambda$ of $H$-degree less than $n$ such that $g \equiv f \mod I_n + I_n$. If $g$ is non-zero, take $\tilde{g}$ to be the homogeneous piece of $g$ of lowest $H$-degree, and write

$$\tilde{g} = w(e_2, e_4, e_6, \ldots).$$

Using (1) we would then get a contradiction to Conjecture 4.1 by taking

$$h(x_3, x_5, \ldots) = w \left( \frac{-x_3}{3}, \frac{-x_5}{5}, \ldots \right).$$

We conclude that $g = 0$, completing the proof. \qed

6. Completed ring of symmetric functions

To study congruences modulo all powers of $p$ at once, it is useful to use the completion $\hat{\Lambda}$ of $\Lambda$ with respect to the grading by $H$-degree: it is the projective limit

$$\hat{\Lambda} := \lim_{\leftarrow} \Lambda/I_n.$$

It is often convenient to view an element of $\hat{\Lambda}$ as a formal infinite sum

$$(7) \quad f = \sum_{n=0}^{\infty} f_n,$$

with $f_n \in \Lambda$ homogeneous of $H$-degree $n$. We define $\hat{I}_k \subset \hat{\Lambda}$ to be the ideal consisting of those $f$ for which $f_n = 0$ for $n < k$. We identify $\Lambda/I_n$ with $\hat{\Lambda}/\hat{I}_n$. 

The maps $\tilde{\varphi}^{[n]} : \Lambda / \mathcal{I}_n \to \mathcal{A}_n$ are compatible with the respective quotient maps, so we get a map

$$\hat{\varphi} : \hat{\Lambda} \to \hat{\mathcal{A}},$$

where $\hat{\mathcal{A}} := \varprojlim_n \mathcal{A}_n$.

We put the discrete topology on each $\mathcal{A}_n$ and $\Lambda / \mathcal{I}_n$ and the projective limit topology on $\hat{\mathcal{A}}$ and $\hat{\Lambda}$, so that $\hat{\varphi}$ is continuous. This means the kernel of $\hat{\varphi}$ is a closed ideal of $\hat{\Lambda}$.

The element $f \in \hat{\Lambda}$ given by (7) is in the kernel of $\hat{\varphi}$ if and only if for all $N \geq 0$ the congruence

$$\sum_{n < N} f_n \left(\frac{p}{1}, \ldots, \frac{p}{p-1}\right) \equiv 0 \mod p^N$$

holds for $p$ sufficiently large.

Proposition 3.1 implies that the elements $\beta_k := e_k + \sum_{j=k}^{\infty} (-1)^{j+1} \binom{j}{k} e_j \in \hat{\Lambda}$

are in the kernel of $\hat{\varphi}$. If we assume Conjecture 4.1, we can show that the $\beta_k$ actually topologically generate ker $\hat{\varphi}$.

**Theorem 6.1.** Assume the truth of Conjecture 4.1. Then the kernel of $\hat{\varphi}$ is equal to the closure of the ideal

$$I_\beta := (\beta_0, \beta_1, \ldots) \subset \hat{\Lambda}.$$

**Proof.** The inclusion $I_\beta \subset \ker \hat{\varphi}$ follows because ker $\hat{\varphi}$ is closed and $\beta_n \in \ker \hat{\varphi}$. For the reverse inclusion, suppose $f \in \ker \hat{\varphi}$. This means that for each $n$ the reduction of $f$ modulo $\mathcal{I}_n$ is in ker $\varphi^{[n]}$. Theorem 5.1 then implies that the reduction of $f$ is in $I^{[n]}$. The preimage of $I^{[n]}$ under the quotient map $\hat{\Lambda} \to \hat{\Lambda} / \mathcal{I}_n$ is $I_\beta + \mathcal{I}_n$, so we have $f \in I_\beta + \mathcal{I}_n$ for all $n$. The ideals $\mathcal{I}_n$ form a neighborhood basis of 0 in $\hat{\Lambda}$, so it follows that $f \in I_\beta$. □

**Remark 6.2.** The ring of symmetric functions has the structure of a Hopf algebra: there is a comultiplication map $\Delta : \Lambda \to \Lambda \otimes \Lambda$ giving $\Lambda$ the structure of a cogroup object in the category of $\mathbb{Q}$-algebras. This induces a cogroup object structure on the topological $\mathbb{Q}$-algebra $\hat{\Lambda}$ (the induced comultiplication $\Delta : \hat{\Lambda} \to \hat{\Lambda} \hat{\otimes} \hat{\Lambda}$ involves the completed tensor product). It can be shown that the closed ideal $I_\beta$ is a Hopf ideal, i.e., the Hopf algebra structure descends to the quotient $\hat{\Lambda} / I_\beta$. The proof of this fact will be given in a later work.

We also show that Conjecture 4.1 implies that every congruence $(\star)$ arises from an element of ker $\hat{\varphi}$ in the following sense:

**Theorem 6.3.** Assume the truth of Conjecture 4.1. Let $n$ be a positive integer, and suppose $f \in \Lambda$ satisfies $(\star)$ and that $f$ has $H$-degree less than $n$. Then there exists

$$g = \sum_{k \geq 0} g_k \in \ker \hat{\varphi} \subset \hat{\Lambda},$$

where

$$\sum_{n < N} f_n \left(\frac{p}{1}, \ldots, \frac{p}{p-1}\right) \equiv 0 \mod p^N.$$
with $g_k$ homogeneous of $H$-degree $k$, such that
\[ f = \sum_{k<n} g_k. \]

Note that the converse of this result is true unconditionally (i.e., the existence of such a $g$ implies that $f$ satisfies ($\ast$)). In [3] (Conjecture 1), we conjecture that an analogous result should hold for quasi-symmetric functions.

**Proof.** By Theorem 5.1, the reduction of $f$ modulo $\mathcal{I}_n$ is in $I^{[n]}$. This means that we can find elements $r_0, \ldots, r_k \in \Lambda / \mathcal{I}_n$ such that
\[ f \equiv r_0 \beta_0^{[n]} + \ldots + r_k \beta_k^{[n]} \mod \mathcal{I}_n. \]
Let $\tilde{r}_0, \ldots, \tilde{r}_k \in \Lambda$ be lifts of $r_0, \ldots, r_k$ (we may choose $\tilde{r}_0, \ldots, \tilde{r}_k \in \Lambda$ to be the unique lifts of $H$-degree less than $n$), and set
\[ g = \tilde{r}_0 \beta_0 + \ldots + \tilde{r}_k \beta_k \in \hat{\Lambda}. \]
Theorem 6.1 implies that $g \in \ker \hat{\varphi}$, and by construction $g \equiv f \mod \mathcal{I}_n$. Finally the hypothesis that $f$ has $H$-degree less than $n$ implies the desired result. \qed

**Acknowledgements**

I thank Jeff Lagarias for many helpful discussion, references, suggestions, and support. This work supported in part by NSF grants DMS-0943832 and DMS-1101373.

**References**

[1] Romeo Meštrović. On the mod $p^7$ determination of $\binom{2p-1}{p-1}$. Rocky Mountain Journal of Mathematics, 2012, arXiv:1108.1174.
[2] Romeo Meštrović. Wolstenholme’s theorem: its generalization and extensions in the last hundred and fifty years (1862-2012). 2012, arXiv:1111.3057v2.
[3] Julian Rosen. Asymptotic relations among multiple harmonic sums, 2013, arXiv:1309.0908.
[4] Julian Rosen. Multiple harmonic sums and wolstenholme’s theorem. International Journal of Number Theory, 2013. To appear.
[5] Roberto Tauraso. More congruences for central binomial coefficients. J. Number Theory, 130(12):2639–2649, 2010.
[6] Jianqiang Zhao. Wolstenholme type theorem for multiple harmonic sums. Int. J. Number Theory, 4(1):73–106, 2008.
[7] Jianqiang Zhao. Mod $p$ structure of alternating and non-alternating multiple harmonic sums. J. Théor. Nombres Bordeaux, 23(1):299–308, 2011.

E-mail address: j2rosen@uwaterloo.ca