International Journal of Number Theory
Vol. 9, No. 8 (2013) 2033–2052
© World Scientific Publishing Company
DOI: 10.1142/S1793042113500735

World Scientific
www.worldscientific.com

MULTIPLE HARMONIC SUMS AND WOLSTENHOLME'S THEOREM

JULIAN ROSEN
Department of Mathematics, University of Michigan
530 Church Street, Ann Arbor, MI 48109, USA
rosenjh@umich.edu

Received 31 January 2013
Accepted 9 June 2013
Published 30 August 2013

We give a family of congruences for the binomial coefficient $\binom{kp-1}{p-1}$, with k an integer and p a prime. Our congruences involve multiple harmonic sums, and hold modulo arbitrary large powers of p. The general congruence in our family, which depends on a parameter n, involves n "elementary symmetric" multiple harmonic sums, and holds modulo p^{2n+3}. These congruences are actually part of a much larger collection of congruences for $\binom{kp-1}{p-1}$ in terms of the elementary symmetric multiple harmonic sums. Congruences in our family have been optimized, in that they involve the fewest multiple harmonic sums among those congruences holding modulo the same power of p. The coefficients in our congruences are given by polynomials in k.

Keywords: Multiple harmonic sums; binomial coefficients.

Mathematics Subject Classification 2010: 11A07, 11B65, 11B73

1. Introduction

In 1862 Wolstenholme [17] noted the congruence that for all primes $p \geq 5$,

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

This result is now known as Wolstenholme's theorem. It was later found that the related congruence on harmonic numbers $H_n := \sum_{j=1}^{n} \frac{1}{j}$, stating that for all primes $p \geq 5$,

$$H_{p-1} \equiv 0 \pmod{p^2},$$

which was discovered earlier (by Waring [15] in 1782 and again by Babbage [1] in 1819), is in fact equivalent to Wolstenholme's result.

In the following 150 years, Wolstenholme's congruence has been generalized in many directions (see [8] for a survey). This paper considers generalizations in two directions. The first direction treats a larger set of binomial coefficients, replacing

$2p-1$ with $kp-1$. An example of this is given by Glaisher [4], who in 1900 showed that for all integers $k \geq 2$,

$$\binom{kp-1}{p-1} \equiv 1 \pmod{p^3} \tag{1.1}$$

holds for all $p \geq 5$.

The second direction obtains congruences modulo higher powers of p, by adding extra terms to the right-hand side of Wolstenholme's congruence. In 2000 Van Hamme [14] proved a result implying that for all primes $p \geq 7$,

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{j=1}^{p-1} \frac{1}{j} \pmod{p^5}, \tag{1.2}$$

where $H_n := \sum_{j=1}^{n} \frac{1}{j}$ are the harmonic numbers. Recently Meštrović [9] showed that for any prime $p \geq 11$,

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{j=1}^{p-1} \frac{1}{j} + 4p^2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} \pmod{p^7}. \tag{1.3}$$

This congruence involves the additional expression

$$\sum_{1 \leq i < j \leq p-1} \frac{1}{ij},$$

which is an example of a multiple harmonic sum, defined below.

The main result of this paper is a simultaneous generalization and unification of these results, giving congruences for $\binom{kp-1}{p-1}$ to arbitrary powers of p.

1.1. *Main result*

A *composition* is a finite ordered list $(s_1, \ldots, s_k)$ of positive integers. For ease of notation, we will denote by $\{s_1, \ldots, s_k\}^a$ the composition

$$(\underbrace{s_1, \ldots, s_k}, \underbrace{s_1, \ldots, s_k}, \ldots, \underbrace{s_1, \ldots, s_k})$$

consisting of a concatenated copies of $(s_1, \ldots, s_k)$.

Definition 1.1. For $\mathbf{s} = (s_1, \ldots, s_k)$ a composition and n a positive integer, we define the *multiple harmonic sum*

$$H_n(\mathbf{s}) := \sum_{n \geq n_1 > \cdots > n_k \geq 1} \frac{1}{n_1^{s_1} \cdot \ldots \cdot n_k^{s_k}}.$$

By convention, we set $H_n(\mathbf{s}) = 0$ if $k > n$.

It has long been known (see, e.g., [7]) that the binomial coefficient $\binom{kp-1}{p-1}$ (for k an integer) can be written as a linear combination of "elementary symmetric" multiple harmonic sums $H_{p-1}(\{1\}^j)$:

$$\binom{kp-1}{p-1} = \sum_{j=0}^{p-1} (k-1)^j p^j H_{p-1}(\{1\}^j).$$

For a fixed non-negative integer n, we may truncate this equation after the $2n$th term and use known results on the p-adic valuation of the multiple harmonic sums $H_{p-1}(\{1\}^j)$ to obtain the congruence

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{2n} (k-1)^j p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}, \tag{1.4}$$

which holds for all primes $p \geq 2n+5$.

In Sec. 2 we derive a family of identities involving the multiple harmonic sums $H_{p-1}(\{1\}^j)$. We use these identities to cancel terms appearing in (1.4). Our main result, like Eq. (1.4), gives for each non-negative integer n a congruence for the binomial coefficient $\binom{kp-1}{p-1}$ mod p^{2n+3}, involving multiple harmonic sums. However, our congruence uses only n elementary symmetric multiple harmonic sums, instead of the $2n$ used in Eq. (1.4).

The coefficients in our congruences are polynomials in k. We make the following definition.

Definition 1.2. Let $0 \leq j \leq n$ be integers. The *extremal polynomial* $b_{j,n}(T) \in \mathbb{Q}[T]$ is the unique polynomial of degree at most $2n+1$ satisfying:

(C1) $b_{j,n}(T) \equiv (T-1)^j \bmod (T-1)^{n+1}$;
(C2) $b_{j,n}(T) \equiv (-1)^j T^j \bmod T^{n+1}$.

A table of the extremal polynomials $b_{j,n}(T)$ for $0 \leq j \leq n \leq 3$ can be found in Sec. 1.2. Now we can state our main result.

Theorem 1.3 (Optimized Congruences). *Let $n \geq 0$ be a fixed integer. The extremal polynomials $b_{j,n}(T)$ $(0 \leq j \leq n)$ have integer coefficients, and for every prime $p \geq 2n+5$ and every integer $k \geq 1$:*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k) p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}. \tag{1.5}$$

This congruence holds mod p^{2n+2} *for* $p = 2n+3$, *and is equality for* $3 \leq p \leq 2n+1$.

Wolstenholme's congruence is the case $n = 0, k = 2$ of Theorem 1.3. As another example, taking $n = k = 3$ gives the congruence

$$\binom{3p-1}{p-1} \equiv 1 + 402pH_{p-1}(1) - 396p^2 H_{p-1}(1,1) + 216p^3 H_{p-1}(1,1,1) \mod p^9.$$

Theorem 1.3 has three important features:

- The coefficients $b_{j,n}(k)$ in the congruence (1.5) are independent of the prime p.
- The congruences may fail to hold (mod p^{2n+3}) for $p = 2n+3$ (when $2n+3$ is prime), and also fail to hold for $p = 2$.
- The extremal polynomials $b_{j,n}(T)$ depend on n, and for fixed j their values at integers $b_{j,n}(k)$, which are the coefficients in the congruences, do *not* stabilize as $n \to \infty$ (with the exception of $b_{0,n}(k)$; see Tables 1 and 2 in Sec. 1.2).

One may ask whether the coefficients $b_{j,n}(k)$ appearing in the extremal congruences (1.5) are uniquely characterized by (1.5) holding for all sufficiently large primes p; we discuss this in Sec. 1.3, where we show that an affirmative answer would follow from the conjecture that there exist infinitely many regular primes.

An *exceptional congruence* will be a triple (k, n, p) such that the corresponding congruence given in Theorem 1.3 holds modulo an extra power of p. We characterize exceptional congruences for primes $p \geq 2n+3$ as follows.

Theorem 1.4 (Exceptional Congruences). *Let n be a non-negative integer, $p \geq 2n+5$ a prime. For all $k \in \mathbb{Z}$, the exceptional congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k) p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+4}}$$

holds if and only if either $k \equiv 0, 1 \pmod{p}$ or p divides the numerator of the Bernoulli number B_{p-2n-3}.

We obtain Theorem 1.3 as special case of a much more general family $\mathcal{F}_{N,k}$ of generalized Wolstenholme congruences, given in Theorem 3.3, and with the $\mathcal{F}_{N,k}$ specified in Definition 3.4. The general congruence in the family $\mathcal{F}_{N,k}$ (which will hold for all sufficiently large primes p) is of the form

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{N} b_j p^j H_{p-1}(\{1\}^j) \pmod{p^{N+1+\epsilon}}, \tag{1.6}$$

where $\epsilon \in \{1, 2\}$ is chosen so that $\epsilon \equiv N \pmod 2$, and the coefficients b_j are rational numbers. Each congruence in this general family is derived from (1.4), using linear combinations of identities among multiple harmonic sums (these identities are stated as Theorem 2.2). The optimized congruence (1.5) is distinguished as the unique congruence in the family $\mathcal{F}_{2n,k}$ satisfying $b_{n+1} = b_{n+2} = \cdots = b_{2n} = 0$.

1.2. *The extremal polynomials $b_{j,n}(T)$*

In Sec. 6 we prove some interesting properties of the extremal polynomials $b_{j,n}(T)$. Table 1 presents data on these polynomials for small j, n.

Table 1. Extremal polynomials $b_{j,n}(T)$.

	j			
n	0	1	2	3
0	1			
1	1	$T^2 - T$		
2	1	$-T^4 + 2T^3 - T$	$T^4 - 2T^3 + T^2$	
3	1	$2T^6 - 6T^5 + 5T^4 - T + 1$	$-2T^6 + 6T^5 - 5T^4 + T^2$	$T^6 - 3T^5 + 3T^4 - T^3$

Table 2. Extremal coefficients $b_{j,n}(k)$ for $k = 2$.

	j					
n	0	1	2	3	4	5
0	1					
1	1	2				
2	1	−2	4			
3	1	14	−12	8		
4	1	−66	68	−40	16	
5	1	382	−380	248	−112	32

Table 1 illustrates that $b_{0,n}(T) = 1$ for all n (this will be established in Sec. 6). While the definition of $b_{j,n}(T)$ given earlier shows that it has degree at most $2n+1$, in fact its degree is at most $2n$ (see Theorem 4.6).

We next consider the coefficients $b_{j,n}(k)$ appearing in the extremal congruences given in Theorem 1.3. Values of the coefficients for $k = 2$ are given in Table 2.

Table 2 shows that $b_{1,2}(2) = -2$, $b_{2,2}(2) = 4$, so that Theorem 1.3 reduces to Meštrović's result (1.3) in the case $n = k = 2$.

1.3. *Uniqueness*

The statement of Theorem 1.3 raises an issue concerning whether the coefficients $b_{j,n}(k)$ above are uniquely determined by the condition that the congruences (1.5) hold for all sufficiently large primes p. We cannot prove this unconditionally. However, we will show that it would follow from a conjecture concerning Bernoulli numbers, which we state here as follows.

Conjecture 1.5 (Linear Bernoulli Nondegeneracy Conjecture). *For all odd integers $k \geq 3$, there exist infinitely many primes p for which p does not divide the numerator of the Bernoulli number B_{p-k}.*

Recall that a prime p is called *regular* if p does not divide the numerators of any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$. It is believed that there are infinitely many regular primes; this would imply Conjecture 1.5. A stronger version of this conjecture was given by Zhao [19].

Theorem 1.6 (Uniqueness of Optimized Congruences). *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture. Let n, k be integers with $n \geq 0$, and suppose $b_0, \ldots, b_n \in \mathbb{Q}$ are such that the congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_j p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}$$

holds for all sufficiently large primes p. Then we have $b_j = b_{j,n}(k)$, where $b_{j,n}(T)$ are the extremal polynomials given by Definition 1.2.

1.4. *Related results*

The literature contains a vast collection of identities and congruences involving multiple harmonic sums and related sums, starting with work of Euler on harmonic numbers. Some of these involve binomial coefficient congruences (see [5] for a survey).

A number of congruences are known for the elementary symmetric multiple harmonic sums $H_n(\{1\}^r)$ considered in this paper. In 1900 Glaisher [3] proved that for all odd $r \geq 5$ and all primes $p \geq 7$,

$$S_r(p) := \frac{pr}{2} H_{p-1}(\{1\}^r) - H_{p-1}(\{1\}^{r-1}) \equiv 0 \pmod{p^4}.$$

In 1953 Carlitz [2] sharpened the congruence of Glaisher to show for all odd $r \geq 5$ and prime $p \geq 7$,

$$S_r(p) \equiv p^4 \frac{(p-r)(p-r-1)(p-r-2)}{24(p-r-3)(p-1)!} B_{p-3} \pmod{p^5},$$

giving a relation with Bernoulli numbers. Along similar lines, Tauraso [13] shows that for any prime $p \geq 7$,

$$\begin{aligned} H_{p-1}(1) &\equiv -\frac{1}{2} p H_{p-1}(1,1) - \frac{1}{6} p^2 H_{p-1}(1,1,1) \\ &\equiv p^2 \left(\frac{B_{2p-5}}{3p-5} - 3\frac{B_{2p-4}}{2p-4} + 3\frac{B_{p-3}}{p-3} \right) + p^4 \frac{B_{p-5}}{p-5} \pmod{p^5}. \end{aligned}$$

Hoffman [6] and Zhao [18] independently investigated congruence properties of multiple harmonic sums mod p (and sometimes mod p^2). The theory of multiple harmonic sums (and particular, their values mod p) is analogous to the study of multiple zeta values. Relations among multiple zeta values have been studied extensively.

The appearance of Bernoulli numbers in these congruences suggest a connection with p-adic zeta functions. Indeed, Morita [10, 11] demonstrated a relation between the power sum multiple harmonic sums $H_{p-1}(n)$ and the Kubota–Leopoldt p-adic L-function. More recent result along these lines are given by Washington [16]. In [12], we provide a family of congruences for $\zeta_p(k)$ in terms of the multiple harmonic sums $H_{p-1}(n)$. These congruences exploit relations among the power sum multiple harmonic sums, and are similar to the congruences in this work.

2. Representing Binomial Coefficients in Terms of Multiple Harmonic Sums

Let n be a positive integer, and define a polynomial

$$f_n(T) := \sum_{j=0}^{n} (n+1)^j H_n(\{1\}^j) T^j \in \mathbb{Q}[T]. \tag{2.1}$$

The coefficients of $f_n(T)$ are the elementary symmetric functions in $\frac{n+1}{1}, \frac{n+1}{2}, \ldots, \frac{n+1}{n}$, so there is a factorization

$$f_n(T) = \prod_{j=1}^{n} \left(1 + \frac{n+1}{j} T\right) = \frac{1}{n!} \prod_{j=1}^{n} ((n+1)T + j). \tag{2.2}$$

This factorization shows that f_n satisfies the functional equation $f_n(-1-T) = (-1)^n f_n(T)$. This gives the equality

$$\begin{aligned}\sum_{j \geq 0} (n+1)^j H_n(\{1\}^j) T^j &= (-1)^n \sum_{j \geq 0} (n+1)^j H_n(\{1\}^j)(-1-T)^j \\ &= \sum_{j \geq 0} (-1)^{n+j} (n+1)^j H_n(\{1\}^j) \sum_{0 \leq i \leq j} \binom{j}{i} T^i \\ &= \sum_{i \geq 0} \left(\sum_{j \geq i} \binom{j}{i} (-1)^{n+j} (n+1)^j H_n(\{1\}^j) \right) T^i,\end{aligned}$$

holding identically in T. Equating the coefficient of T^j on each side and rearranging gives the following identity.

Proposition 2.1. *For all non-negative integers n, j, we have*

$$(n+1)^j H_n(\{1\}^j) + \sum_{i \geq j} (-1)^{n+i+1} \binom{i}{j} (n+1)^i H_n(\{1\}^i) = 0. \tag{2.3}$$

The sum above is finite, as the terms corresponding to $i > n$ vanish. We thus have a family of linear equations (indexed by j) satisfied by the quantities $(n+1)^i H_n(\{1\}^i)$, $i = 0, 1, \ldots, n$.

Next we obtain a general set of identities expressing binomial coefficients in terms of the $H_n(\{1\}^j)$.

Proposition 2.2. *Let n be a non-negative integer, k, $c_0, c_1, \ldots$ be indeterminates, and define*

$$b_j = (k-1)^j + c_j + (-1)^{n+j+1} \sum_{i=0}^{j} \binom{j}{i} c_i. \tag{2.4}$$

Then the equation

$$\binom{k(n+1)-1}{n} = \sum_{j=0}^{\infty} b_j (n+1)^j H_n(\{1\}^j) \tag{2.5}$$

holds identically in the indeterminates k, $c_0, c_1, \ldots$. Here the right-hand side of (2.5) *is a finite sum, since $H_n(\{1\}^j) = 0$ for $j > n$.*

Proof. We begin by using Eqs. (2.1) and (2.2) to write

$$\begin{aligned}\binom{k(n+1)-1}{n} &= f_n(k-1)\\ &= \sum_{j\geq 0}(k-1)^j(n+1)^j H_n(\{1\}^j).\end{aligned}$$

We add to this equation a linear combination of Eq. (2.3) (where c_j is the coefficient of the equation indexed by j) to obtain the general formula. □

Remark 2.3. By making suitable choices of the parameters c_i in Proposition 2.2, we can arrange to have $b_j = 0$ for many j. Theorem 4.1 is obtained by optimizing this process.

3. Congruences for $\binom{kp-1}{p-1}$ Modulo Powers of p

To obtain congruences for $\binom{kp-1}{p-1}$, we will truncate the expansion of Proposition 2.2, with k an integer and $n = p-1$, p an odd prime. To establish a bound on the error due to truncation, we need some congruence properties of multiple harmonic sums.

3.1. *Congruence properties of multiple harmonic sums*

Zhao [18, Theorem 1.6] gives the following congruence involving multiple harmonic sums $H_{p-1}(\{1\}^j)$ and Bernoulli numbers.

Proposition 3.1. *Let p be a fixed odd prime, and j be an integer with $1 \leq j \leq p-3$. Then we have*

$$H_{p-1}(\{1\}^j) \equiv \begin{cases} \dfrac{-B_{p-1-j}}{j+1}p \pmod{p^2} & \text{if } j \equiv 0 \mod 2,\\ \left(\dfrac{-(j+1)}{2(j+2)}B_{p-2-j}\right)p^2 \pmod{p^3} & \text{if } j \equiv 1 \mod 2.\end{cases}$$

We prove an additional congruence for $H_{p-1}(\{1\}^j))$ for those j which are not covered by Proposition 3.1.

Proposition 3.2. *Let p be a fixed odd prime, and j be a positive integer.*

(1) *If $j = p-2$ we have $H_{p-1}(\{1\}^j) \equiv \frac{1}{2}p \pmod{p^2}$.*
(2) *If $j = p-1$ we have $H_{p-1}(\{1\}^j)) \equiv -1 \pmod{p}$.*
(3) *If $j \geq p$ we have $H_{p-1}(\{1\}^j) = 0$.*

Proof. (1) We have

$$H_{p-1}(\{1\}^{p-2}) = \sum_{i=1}^{p-1}\frac{1}{1\cdots\hat{\imath}\cdots(p-1)}$$

$$\begin{aligned}&= \frac{1}{(p-1)!}\sum_{i=1}^{p-1} i\\ &= \frac{1}{(p-1)!}\frac{p(p-1)}{2}\\ &\equiv \frac{p}{2} \pmod{p^2}.\end{aligned}$$

In the last line, we used Wilson's theorem, stating that $(p-1)! \equiv -1 \pmod{p}$.

(2) We have

$$\begin{aligned}H_{p-1}(\{1\}^{p-1}) &= \frac{1}{(p-1)!}\\ &\equiv -1 \pmod{p}.\end{aligned}$$

(3) For $j \geq p$ the defining sum is empty. □

3.2. *A general family of congruences*

We can now obtain our general family of congruences for $\binom{kp-1}{p-1}$. The congruences are obtained from Proposition 2.2 by truncation. We take some care to express the error due to truncation in terms of Bernoulli numbers.

Theorem 3.3 (General Wolstenholme-Like Congruence). *Let k be an integer. Let $c_0, c_1, \ldots \in \mathbb{Q}$ be given, and take $b_j \in \mathbb{Q}$ to be*

$$b_j := (k-1)^j + c_j + (-1)^{j+1}\sum_{i=0}^{j}\binom{j}{i}c_i. \tag{3.1}$$

Fix an odd prime p not dividing the denominator of any c_i, and let N be a nonnegative integer. Define

$$E_N := \binom{kp-1}{p-1} - \sum_{j=0}^{N} b_j p^j H_{p-1}(\{1\}^j).$$

(i) *If $0 \leq N \leq p-4$, then*

$$E_N \equiv \begin{cases} \dfrac{-B_{p-3-N}}{N+3}\left(\dfrac{N+2}{2}b_{N+1} + b_{N+2}\right)p^{N+3} & \pmod{p^{N+4}} \textit{ if } N \textit{ is even},\\[2ex] \dfrac{-B_{p-2-N}}{N+2}b_{N+1}p^{N+2} & \pmod{p^{N+3}} \textit{ if } N \textit{ is odd}.\end{cases}$$

(ii) *If $N = p-3$, then $E_N \equiv (\frac{b_{N+1}}{2} - b_{N+2})p^{N+2} \pmod{p^{N+3}}$.*

(iii) *If $N = p-2$, then $E_N \equiv -b_{N+1}p^{N+1} \pmod{p^{N+2}}$.*

(iv) *If $N \geq p-1$, then $E_N = 0$.*

In particular, we get the congruence

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{N} b_j p^j H_{p-1}(\{1\}^j) \quad \begin{cases} \bmod p^{N+3} & \text{if } N \le p-4,\ N \text{ even},\\ \bmod p^{N+2} & \text{if } N \le p-4,\ N \text{ odd},\\ \bmod p^{N+2} & \text{if } N = p-3,\\ \bmod p^{N+1} & \text{if } N = p-2,\\ \bmod 0 & \text{if } N \ge p-1. \end{cases} \tag{3.2}$$

(*Congruence* mod 0 *means equality.*)

Proof. We apply Proposition 2.2 with $n = p-1$ to obtain the equality

$$\binom{kp-1}{p-1} = \sum_{j=0}^{\infty} b_j p^j H_{p-1}(\{1\}^j).$$

Because $n = p-1$ is even, the values of b_i do not depend on p. The b_j are p-integral (because we assume the c_j to be p-integral), as are the multiple harmonic sums $H_{p-1}(\{1\}^j)$, so we have

$$E_N \equiv \sum_{j=N+1}^{N+3} b_j p^j H_{p-1}(\{1\}^j) \pmod{p^{N+4}}.$$

Case (i-a). Suppose $0 \le N \le p-5$ and N is even. Propositions 3.1 and 3.2 imply $H_{p-1}(\{1\}^{N+1}) \equiv \frac{-(N+2)}{2(N+3)} B_{p-3-N} p^2 \pmod{p^3}$, $H_{p-1}(\{1\}^{N+2}) \equiv \frac{-1}{N+3} B_{p-N-3} p \pmod{p}$, and $H_{p-1}(\{1\}^{N+3}) \equiv 0 \pmod{p}$. This implies

$$E_N \equiv \frac{-B_{p-3-N}}{N+3}\left(\frac{N+2}{2} b_{N+1} + b_{N+2}\right) p^{N+3} \pmod{p^{N+4}}.$$

Case (i-b). Suppose $1 \le N \le p-4$ and N is odd. Proposition 3.1 implies $H_{p-1}(\{1\}^{N+1}) \equiv \frac{-1}{N+2} B_{p-2-N} p \pmod{p^2}$ and $H_{p-1}(\{1\}^{N+2}) \equiv 0 \pmod{p}$. This implies

$$E_N \equiv \frac{-B_{p-2-N}}{N+2} b_{N+1} p^{N+2} \pmod{p^{N+3}}.$$

Case (ii). Suppose $N = p-3$. Proposition 3.2 implies $H_{p-1}(\{1\}^{p-2}) \equiv \frac{p}{2} \pmod{p^2}$, $H_{p-1}(\{1\}^{p-1}) \equiv -1 \pmod{p}$, so

$$E_N \equiv \left(\frac{b_{N+1}}{2} - b_{N+2}\right) p^{N+2} \pmod{p^{N+3}}.$$

Case (iii). Suppose $N = p-2$. Proposition 3.2 implies $H_{p-1}(\{1\}^{p-1}) \equiv -1 \pmod{p}$, so

$$E_N \equiv -b_{N+1} p^{N+1} \pmod{p^{N+2}}.$$

Case (iv). Suppose $N \geq p-1$. Then E_N is given by an empty sum, so $E_N = 0$. □

Definition 3.4. We call the congruence (3.2) the *generalized Wolstenholme congruence* associated with the data

$$[k, (c_0, c_1, \ldots), N],$$

and we will say that $b_0, \ldots, b_N$ are the *generalized Wolstenholme coefficients* associated with this data. We let $\mathcal{F}_{N,k}$ denote the family of all generalized Wolstenholme congruences above, where N, k are fixed and the other data varies.

Assuming the truth of the Linear Bernoulli Nondegeneracy Conjecture, we can show that our family contains *all* congruences of this form.

Theorem 3.5 (Strong Uniqueness). *Assume the truth of the Linear Bernoulli Nondegeneracy Conjecture. If k, m are integers with $m \geq 0$, and $a_0, \ldots, a_n \in \mathbb{Q}$ are such that*

$$\binom{kp-1}{p-1} \equiv a_0 + a_1 pH(\{1\}^1) + \cdots + a_n p^n H(\{1\}^n) \pmod{p^m}$$

holds for all but finitely many p, then this congruence arises from Theorem 3.3, *in the following sense*: *there are constants $c_0, c_1, \ldots \in \mathbb{Q}$ such that, if $b_0, b_1, \ldots$ are defined by* (3.1), *then we have $a_i = b_i$ for $i = 0, 1, \ldots, \psi(m)$, where $\psi(m) = m-2$ if m is even and $\psi(m) = m-3$ if m is odd.*

Proof. Suppose, to the contrary, that there is a congruence of the form

$$\binom{kp-1}{p-1} \equiv a_0 + a_1 pH(\{1\}^1) + \cdots + a_n p^n H(\{1\}^n) \pmod{p^m},$$

holding for sufficiently large p, which does not arise from Theorem 3.3. Subtracting the identity

$$\binom{kp-1}{p-1} = \sum_{j \geq 0} (k-1)^j p^j H_{p-1}(\{1\}^j)$$

from this congruence gives us a congruence of the form

$$\sum_{j \geq 0} c_j p^j H_{p-1}(\{1\}^j) \equiv 0 \pmod{p^m}, \tag{3.3}$$

which by hypothesis does not arise from truncating a linear combination of the identities (2.3). We may choose (3.3) so that $j_0 := \min\{j : c_j \neq 0\}$ is maximized among all congruences of this shape not arising from a truncation of a linear combinations of the identities (2.3). This implies that j_0 is even, for if j_0 were odd, we could add $\frac{-1}{2} c_j$ times the identity (2.3) with $j = j_0$, canceling the lowest-order term and contradicting the maximality of j_0. By hypothesis, we also have $m \geq j_0 + 2$, so by reducing (3.3) mod p^{j_0+2}, we get

$$c_{j_0} p^{j_0} H_{p-1}(\{1\}^{j_0}) \equiv 0 \pmod{p^{j_0+2}}$$

for all sufficiently large primes p. Using Proposition 3.1, we get

$$\frac{c_{j_0}}{j_0+1} p^{j_0+1} B_{p-1-j_0} \equiv 0 \pmod{p^{j_0+2}}$$

for all sufficiently large p. Since $c_{j_0} \neq 0$, this contradicts the Linear Bernoulli Nondegeneracy Conjecture. □

Remark 3.6. For fixed k, N, the family $\mathcal{F}_{N,k}$ has the structure of an affine linear space over $\mathbb{Q}$ in the following way: if $B = (b_0, \ldots, b_N)$ and $B' = (b'_0, \ldots, b'_N)$ are the coefficients associated with the data $[k, (c_0, c_1, \ldots), N]$, $[k, (c'_0, c'_1, \ldots), N]$ respectively, and $t \in \mathbb{Q}$, then

$$tB + (1-t)B' = (tb_0 + (1-t)b'_0, \ldots, tb_N + (1-t)b'_N),$$

where the numbers on the right-hand side are the generalized Wolstenholme coefficients associated with the data

$$[k, (tc_0 + (1-t)c'_0, tc_1 + (1-t)c'_1, \ldots), N].$$

In the next section we will focus exclusively on the case where $N = 2n$ is even. We will determine that the affine space of generalized Wolstenholme coefficients, for arbitrary k and $N = 2n$, has dimension n.

Now we consider some special cases of Theorem 3.3. In what follows we will write $(c_0, \ldots, c_m)$ for the sequence $(c_0, \ldots, c_m, 0, 0, \ldots)$.

As one example, fix a positive integer k and take the data $[k, ((k-1)^2), 2]$. This gives $(b_0, b_1, b_2, b_3, b_4) = (1, k(k-1), 0)$, so we get the congruence.

Corollary 3.7. *For all integers k and all primes $p \neq 2, 5$, we have*

$$\binom{kp-1}{p-1} \equiv 1 + k(k-1)pH_{p-1}(1) \pmod{p^5}.$$

This is a generalization of Van Hamme's result (1.2). Taking the data $[2, (49, -18, 4), 6]$ gives $(b_0, b_1, \ldots, b_6) = (1, 14, -12, 8, 0, 0, 0)$, so we get the following.

Corollary 3.8. *For all odd primes p, we have*

$$\binom{2p-1}{p-1} \equiv 1 + 14pH_{p-1}(1) - 12p^2 H_{p-1}(1,1) + 8p^3 H_{p-1}(1,1,1) \pmod{p^9}.$$

Corollaries 3.7 and 3.8 are special cases of Theorem 3.3.

4. Optimized Binomial Congruences

We now state a version of our main result (Theorem 1.3). We show that when $N = 2n$ is even, it is always possible to choose the data $(c_0, c_1, \ldots)$ so that $b_{n+1} =$

$b_{n+2} = \cdots = b_{2n} = 0$. Moreover, this condition will uniquely determine the values of b_j for $0 \leq j \leq n$. We will derive this result using Theorem 3.3.

Theorem 4.1 (Optimized Binomial Congruences). *Let integers k, n be given, with $n \geq 0$, and set $N = 2n$. There is a unique generalized binomial congruence whose coefficients $b_0, \ldots, b_{2n}$ satisfy $b_{n+1} = b_{n+2} = \cdots = b_{2n} = 0$. This congruence has $b_0, b_1, \ldots, b_n \in \mathbb{Z}$.*

In other words, for $N = 2n$, Theorem 3.3 *produces a unique congruence of the form*

$$\binom{kp-1}{p-1} \equiv b_0 + b_1 pH(1) + \cdots + b_n p^n H(\{1\}^n) \pmod{p^{2n+3}}, \tag{4.1}$$

with $b_i \in \mathbb{Z}$, which holds for all odd primes $p \neq 2n+3$. This congruence holds mod p^{2n+2} *when $p = 2n+3$, and is equality for $3 \leq p \leq 2n+1$.*

Before giving the proof, we remark that this theorem, combined with Theorem 3.5, implies the uniqueness statement Theorem 1.6.

For the proof of Theorem 4.1, we need some preliminaries.

Definition 4.2. Fix integers N, k, with $N \geq 0$. Define $V_{N,k} \subset \mathbb{Z}^{N+1}$ to be the set

$$V_{N,k} := \Bigg\{ (b_0, \ldots, b_N) : \exists\, c_0, c_1, \ldots \in \mathbb{Z} \\ \text{s.t. } b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \Bigg\}.$$

In other words $V_{N,k}$ is the set of *generalized Wolstenholme coefficients* corresponding to integer data. We similarly define $V_{N,k}^{\mathbb{Q}} \subset \mathbb{Q}^{N+1}$ to be

$$V_{N,K}^{\mathbb{Q}} := \Bigg\{ (b_0, \ldots, b_N) : \exists\, c_0, c_1, \ldots \in \mathbb{Q} \\ \text{s.t. } b_j = (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \Bigg\},$$

the set of generalized Wolstenholme coefficients corresponding to rational data.

The inclusion $V_{N,k} \hookrightarrow V_{N,k}^{\mathbb{Q}}$ induces an isomorphism

$$V_{N,k} \otimes \mathbb{Q} \cong V_{N,k}^{\mathbb{Q}}$$

of affine spaces over $\mathbb{Q}$. We have that $V_{N,k}$ is a coset of the subgroup

$$\hat{V}_N := \left\{ (b_0, \ldots, b_N) : \exists\, c_0, c_1, \ldots \in \mathbb{Z} \text{ s.t. } b_j = c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \right\} \subseteq \mathbb{Z}^N,$$

which does not depend on k. We then have the following.

Proposition 4.3. *For all integers N, k, with $N \geq 0$, we have $V_{N,k} = V_{N,1-k}$.*

Proof. As $V_{N,k}$ and $V_{N,1-k}$ are cosets of the same subgroup $\hat{V}_N \leq \mathbb{Z}^{N+1}$, equality will follow if we can show $V_{N,k} \cap V_{N,1-k} \neq \phi$.

Taking $c_0 = c_1 = \cdots = 0$, we see $(1, (-k), (-k)^2, \ldots, (-k)^N) \in V_{N,1-k}$. To see that this element is also in $V_{N,k}$, set $c_j = -(k-1)^j$. Then

$$\begin{aligned} b_j &= (k-1)^j + c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i \\ &= (k-1)^j - (k-1)^j + (-1)^j \sum_{i=0}^{j} \binom{j}{i} (k-1)^i \\ &= (-k)^j. \end{aligned}$$

□

Lemma 4.4. *For positive integers b, n, $n \times n$ matrix*

$$M_{n,b} := \left(\binom{b+i}{j} \right)_{0 \leq i,j < n}$$

has determinant 1.

Proof. Define $n \times n$ matrices $L_n = (\binom{i}{j})$, $U_{n,b} = (\binom{b}{j-i})$. L_n is unipotent lower-triangular and $U_{n,b}$ is unipotent upper-triangular, so both have determinant 1. It follows from the Vandermonde convolution identity that $M_{n,b} = L_n U_{n,b}$, so that $\det M_{n,b} = (\det L_n)(\det U_{n,b}) = 1$. □

Lemma 4.5. *For all non-negative integers n, $\hat{V}_{2n}$ is a free $\mathbb{Z}$-module of rank n, and the map $\pi : \hat{V}_{2n} \to \mathbb{Z}^n$, $(b_0, \ldots, b_{2n}) \mapsto (b_{n+1}, \ldots, b_{2n})$ is an isomorphism.*

Proof. Here $(b_0, \ldots, b_{2n}) \in \hat{V}_{2n}$ is determined by the values of c_j for $0 \leq j \leq 2n$. We therefore have a surjective map $\varphi_n : \mathbb{Z}^{2n+1} \to \hat{V}_{2n} \leq \mathbb{Z}^{2n+1}$, taking $(c_0, \ldots, c_{2n})$ to $(a_0, \ldots, a_{2n})$ with

$$a_j = c_j + (-1)^{j+1} \sum_{i=0}^{j} \binom{j}{i} c_i.$$

With respect to the standard basis on $\mathbb{Z}^{2n+1}$, φ_n is given by the matrix

$$A_n := \left(\delta_{i,j} + (-1)^{j+1} \binom{j}{i} \right)_{0 \leq i,j \leq 2n}.$$

Let us identify column vectors of length $2n+1$ with the set of polynomials of degree at most $2n$ via the identification $(a_0, \ldots, a_{2n}) \leftrightarrow a_0 + a_1 T + \cdots + a_{2n} T^{2n}$. The jth column of A_n is identified with the polynomial $T^j - (-1-T)^j$. This means that the column span of A_n is contained in the set of polynomials $f(T)$ satisfying $f(T) = -f(-1-T)$. Such polynomials can be written as $\mathbb{Q}$-linear combinations of $T + \frac{1}{2}, (T + \frac{1}{2})^3, \ldots, (T + \frac{1}{2})^{2n-1}$. It follows that $\operatorname{rank}(\hat{V}_{2n}) = \operatorname{rank}(A_n) \leq n$.

Next let $i : \mathbb{Z}^n \to \mathbb{Z}^{2n+1}$, $(x_0, \ldots, x_{n-1}) \mapsto (x_0, \ldots, x_{n-1}, 0, \ldots, 0)$. We have $\pi \circ \varphi_n \circ i(x_0, \ldots, x_{n-1}) = (y_0, \ldots, y_{n-1})$, where

$$y_j = (-1)^{n+j} \sum_{i=0}^{n-1} \binom{n+1+j}{i} x_i.$$

Lemma 4.4 implies this map is bijective. It follows that π is surjective. Since $\operatorname{rank}(\hat{V}_{2n}) \leq n = \operatorname{rank}(\mathbb{Z}^n)$, we must have that $\operatorname{rank}(\hat{V}_{2n}) = n$, and π is bijective.

□

Proof of Theorem 4.1. We need to show that there is a unique element of the form $(b_0, \ldots, b_n, 0, \ldots, 0)$ in $V_{2n,k}^{\mathbb{Q}}$, and that $b_0, \ldots, b_n \in \mathbb{Z}$. It suffices to show there is a unique element of this form in $V_{2n,k}$. Because $V_{2n,k} = (1, (k-1), \ldots, (k-1)^{2n}) + \hat{V}_{2n}$, this is equivalent to the existence of a unique element

$$\underline{a} = (a_0, \ldots, a_n, -(k-1)^{n+1}, \ldots, -(k-1)^{2n})$$

in $\hat{V}_{2n}$. This follows from Lemma 4.5, which implies there is a unique $\underline{a} \in \hat{V}_{2n}$ with $\pi(\underline{a}) = (-(k-1)^{n+1}, \ldots, -(k-1)^{2n})$.

That the values $b_{j,n}(k)$ agree with a polynomial in k will follow from Corollary 4.6 below. □

We summarize the recipe for constructing the coefficients $b_{j,n}(k)$ given in Theorem 4.1. It will follow that these coefficients are interpolated by a polynomial $b_{j,n}(T)$.

Theorem 4.6. *The coefficients $b_{j,n}(k)$ given in Theorem* 4.1 *are values of a polynomial $b_{j,n}(T)$ at $T = k$, having integer coefficients and degree at most $2n$. This polynomial can be computed explicitly as follows.*

Let M_n be the $n \times n$ matrix

$$M_n = \left[(-1)^{n+i} \binom{n+1+i}{j} \right]_{0 \leq i,j \leq n-1}.$$

Let D_n be the $(n+1) \times n$ matrix

$$D_n = \left[(-1)^{i+1} \binom{i}{j} + \delta_{i,j} \right]_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n-1}},$$

where $\delta_{i,j}$ is the Kronecker delta. Then M_n is invertible over the integers, and we have the matrix equation

$$\begin{pmatrix} b_{0,n}(k) \\ b_{1,n}(k) \\ \vdots \\ b_{n,n}(k) \end{pmatrix} = \begin{pmatrix} (k-1)^0 \\ (k-1)^1 \\ \vdots \\ (k-1)^n \end{pmatrix} - D_n \cdot M_n^{-1} \cdot \begin{pmatrix} (k-1)^{n+1} \\ (k-1)^{n+2} \\ \vdots \\ (k-1)^{2n} \end{pmatrix}. \tag{4.2}$$

Definition 4.7. For integers j, n, k, with $j, n \geq 0$, we let $b_{j,n}(k)$ denote the coefficients arising from Theorem 4.1. We call these *extremal coefficients.* We also denote by $b_{j,n}(T)$ the polynomial giving these coefficients, and call these *extremal polynomials.* By convention, we take $b_{j,n}(T) = 0$ for $n+1 \leq j \leq 2n$, and we say that $b_{j,n}(T)$ is not defined for $j \geq 2n+1$.

Proposition 4.3 says that $V_{2n,k} = V_{2n,1-k}$, so we observe that $b_{j,n}(k) = b_{j,n}(1-k)$. Combined with Theorem 4.6, this observation gives the following characterization of the extremal polynomials $b_{j,n}(T)$.

Proposition 4.8. *Fix integers j, n, with $j \leq 2n$. The extremal polynomial $b_{j,n}(T) \in \mathbb{Z}[T]$ is the unique polynomial of degree at most $2n$ satisfying the following conditions*:

(1) $b_{j,n}(T) \equiv (T-1)^j \bmod (T-1)^{n+1}$;
(2) $b_{j,n}(T) \equiv (-T)^j \bmod T^{n+1}$.

Theorem 1.3, stated in Sec. 1, now follows from the combination of Theorem 4.1, Theorem 4.6, and Proposition 4.8.

5. Exceptional Congruences and Bernoulli Numbers

We now investigate the situations under which our congruences hold modulo some larger power of p than given by Theorem 4.1. We term these *exceptional congruences.* In the case of Wolstenholme's theorem, the exceptional congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$$

holds if and only if p divides the numerator of the Bernoulli number B_{p-3}; this follows from results of Van Hamme [14] and Glaisher [3]. We establish a similar result, which shows that the congruence (4.1) holds modulo an extra power of p if and only if either $p|B_{p-2n-3}$, or $p|k(k-1)$.

Fix non-negative integers n, k, and let $c_0, c_1, \ldots \in \mathbb{Z}$ be chosen so that the generalized Wolstenholme congruence associated with the data $[k, (c_0, c_1, \ldots), 2n]$ is the optimal one, given by Theorem 4.1. The c_i are not uniquely determined by this condition. Let $b_0, b_1, \ldots, b_{2n+2}$ be given by (3.1), so that $b_j = b_{j,n}(k)$ for $j = 0, 1, \ldots, n$, and $b_j = 0$ for $j = n+1, n+2, \ldots, 2n$. The values of b_{2n+1} and b_{2n+2} will depend on the choice of the c_i.

Lemma 5.1. *Independent of the choice of c_i, we have*

$$(n+1)b_{2n+1} + b_{2n+2} = k^{n+1}(k-1)^{n+1}.$$

Proof. First we show that the value of $C_n(k)$ depends only on n and k, but not the choice of c_i. Let $\pi : V_{2n+2,k} \to V_{2n,k}$, $(b_0, \ldots, b_{2n+2}) \mapsto (b_0, \ldots, b_{2n})$ be the projection map, which is surjective (where $V_{\cdot,k}$ is given by Definition 4.2). Lemma 4.5 implies that $\operatorname{rank}(V_{2n+2,k}) = n+1$, $\operatorname{rank}(V_{2n,k}) = n$, so that

$U := \pi^{-1}(b_0, b_1, \dots, b_n, 0, \dots, 0)$ is a $\mathbb{Z}$-torsor. We will be done if we can exhibit $(b'_0, \dots, b'_{2n+2}) \neq (b_0, \dots, b_{2n+2}) \in U$ such that $(n+1)b'_{2n+1} + b'_{2n+2} = (n+1)b_{2n+1} + b_{2n+2}$.

If we take $c'_i = c_i$ for $i \neq 2n+1$, and $c'_{2n+1} = c_{2n+1} + 1$, we will have that $b'_i = b_i$ for $i \leq 2n$, $b'_{2n+1} = b_{2n+1} + \binom{2n+1}{1}$, and $b'_{2n+2} = b_{2n+2} - \binom{2n+2}{2}$. It follows directly that $(n+1)b'_{2n+1} + b'_{2n+2} = (n+1)b_{2n+1} + b_{2n+2}$.

Next we show that $C_n(k)$ agrees with a polynomial in k. Using the same process as in Corollary 4.6, we may solve for the data $c_0, \dots, c_{2n}$ to give the extremal congruence. We will use this data (with $c_i = 0$ for $i \geq 2n+1$). We can then compute b_{2n+1}, b_{2n+2} in the following way.

Let M_n be the $n \times n$ matrix

$$M_n = \left[(-1)^{n+i}\binom{n+1+i}{j}\right]_{0 \leq i,j \leq n-1}.$$

Let A_n be the $2 \times n$ matrix

$$A_n = \left[(-1)^{i+1}\binom{i}{j} + \delta_{i,j}\right]_{\substack{2n+1 \leq i \leq 2n+2 \\ 0 \leq j \leq n-1}}.$$

Then M_n is invertible over the integers, and we have the matrix equation

$$\begin{pmatrix} b_{2n+1} \\ b_{2n+2} \end{pmatrix} = \begin{pmatrix} (k-1)^{2n+1} \\ (k-1)^{2n+2} \end{pmatrix} - A_n \cdot M_n^{-1} \cdot \begin{pmatrix} (k-1)^{n+1} \\ (k-1)^{n+2} \\ \vdots \\ (k-1)^{2n} \end{pmatrix}. \tag{5.1}$$

This shows that b_{2n+1}, b_{2n+2} are polynomials in k. Moreover, b_{2n+1} is equal to $(k-1)^{2n+1}$ plus a $\mathbb{Z}$-linear combination of $(k-1)^{n+1}, \dots, (k-1)^{2n}$, so that b_{2n+1} is monic in k, of degree $2n+1$, and $(k-1)^{n+1} | b_{2n+1}$. Similarly, b_{2n+2} is monic of degree $2n+2$, and $(k-1)^{n+1} | b_{2n+2}$. It follows that $C_n(k) = (n+1)b_{2n+1} + b_{2n+2}$ is monic of degree $2n+2$, with $(k-1)^{2n+1} | C_n(k)$. Moreover, $C_n(k)$ is determined by the set $V_{2n+2,k}$, and Lemma 4.3 says that $V_{2n+2,k} = V_{2n+2,1-k}$. We may therefore make the substitution $k \leftrightarrow 1-k$ to get the $k^{n+1} | C_n(k)$. By the Chinese Remainder Theorem, $k^{n+1}(k-1)^{n+1} | C_n(k)$. The only monic polynomial of degree $2n+2$ which is divisible by $k^{n+1}(k-1)^{n+1}$ is $k^{n+1}(k-1)^{n+1}$, so we conclude $C_n(k) = k^{n+1}(k-1)^{n+1}$. □

We now consider the possibility of extra powers of p in the congruence (4.1). For all integers k, n with $n \geq 0$, and all odd primes p, define

$$E(k, n, p) := \binom{kp-1}{p-1} - \sum_{j=0}^{n} b_{j,n}(k) p^j H_{p-1}(\{1\}^j).$$

Proposition 5.2. *Suppose $p \geq 2n+5$. Then*

$$E(k, n, p) \equiv \frac{-B_{p-3-2n}}{2n+3} k^{n+1}(k-1)^{n+1} p^{2n+3} \pmod{p^{2n+4}}.$$

Proof. By Theorem 3.3 and Proposition 3.1, we have

$$\begin{aligned} E(k,n,p) &\equiv b_{2n+1}p^{2n+1}H_{p-1}(\{1\}^{2n+1}) + b_{2n+2}p^{2n+2}H_{p-1}(\{1\}^{2n+2}) \\ &\equiv -b_{2n+1}p^{2n+3}\frac{2n+2}{2(2n+3)}B_{p-3-2n} - b_{2n+2}p^{2n+3}\frac{B_{p-3-2n}}{2n+3} \\ &\equiv \frac{-B_{p-3-2n}}{n+3}((n+1)b_{2n+1} - b_{2n+2}) \\ &\equiv \frac{-B_{p-3-2n}}{n+3}k^{n+1}(k-1)^{n+1} \pmod{p^{2n+4}}. \end{aligned}$$

□

Proposition 5.3. *Suppose $p = 2n+3$. Then*

$$E(k,n,p) \equiv -k^{n+1}(k-1)^{n+1}p^{2n+2} \pmod{p^{2n+3}}.$$

Proof. Using Theorem 3.3 and Proposition 3.1, we have

$$\begin{aligned} E(k,n,p) &= b_{2n+1}p^{2n+1}H_{p-1}(\{1\}^{2n+1}) + b_{2n+2}p^{2n+2}H_{p-1}(\{1\}^{2n+2}) \\ &\equiv \frac{b_{2n+1}}{2}p^{2n+2} - b_{2n+2}p^{2n+2} \\ &\equiv \left(-\frac{(p-1)b_{2n+1}}{2} - b_{2n+1}\right)p^{2n+2} \\ &\equiv -((n+1)b_{2n+1} + b_{2n+2}) \\ &\equiv -k^{n+1}(k-1)^{n+1}p^{2n+2} \pmod{p^{2n+3}}. \end{aligned}$$

□

We can now state the precise conditions under which the congruence in Theorem 4.1 holds modulo an extra power of p. Our next theorem is an immediate consequence of the preceding two propositions.

Theorem 5.4. *Let $n \geq 0$, k be integers, p be an odd prime, and $b_{j,n}(T)$ be the extremal polynomials (characterized by Proposition 4.8).*

(1) *Suppose $p \geq 2n+5$. The congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k)p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+4}}$$

holds if and only if either $p | B_{p-3-2n}$ or $k \equiv 0, 1 \pmod{p}$.

(2) *Suppose $p = 2n+3$. The congruence*

$$\binom{kp-1}{p-1} \equiv \sum_{j=0}^{n} b_{j,n}(k)p^j H_{p-1}(\{1\}^j) \pmod{p^{2n+3}}$$

holds if and only if $k \equiv 0, 1 \pmod{p}$.

6. Properties of the Extremal Polynomials

The extremal polynomials $b_{j,n}(T)$ satisfy many arithmetic conditions. The following proposition records some of these, which follow from Proposition 4.8.

Proposition 6.1. *The extremal polynomials $b_{j,n}(T)$ satisfy the following properties*:

(1) *For all non-negative integers n, $b_{0,n}(T) = 1$ and $b_{n,n}(T) = T^n(T-1)^n$.*
(2) *For all non-negative integers $j \leq 2n$, $T^j(T-1)^j$ divides $b_{j,n}(T)$.*

For fixed j, the polynomials $b_{j,n}(T)$ depend on n. One exception to this is that $b_{0,n}(T) = 1$ for all non-negative integers n. Examining the table in Sec. 1.2, we see that $b_{1,n}(T)$ does indeed depend on n. However, $b_{1,n}(T) + b_{2,n}(T) = T^2 - T$ for all n. This is the first in a family of equations giving linear combinations of the extremal polynomials $b_{j,n}(T)$ which are independent of n.

Proposition 6.2. *Let m be a non-negative integer. Suppose $f(T) = \sum_{j=0}^{m} a_j T^j \in \mathbb{Q}[T]$ satisfying $f(T) = f(-1-T)$. Then for all non-negative integers n with $2n \geq m$, we have*

$$\sum_{j=0}^{m} a_j b_{j,n}(T) = f(T-1).$$

Proof. Define $g(T) = \sum_{j=0}^{m} a_j b_{j,n}(T)$. By Proposition 4.8, $b_{j,n}(T) \equiv (T-1)^j \pmod{(T-1)^{n+1}}$, so that $g(T) \equiv f(T-1) \bmod (T-1)^{n+1}$. Similarly, by Proposition 4.8, $b_{j,n}(T) \equiv (-T)^j \pmod{T^{n+1}}$, so that $g(T) \equiv f(-T) \equiv f(T-1) \bmod T^{n+1}$. This means $g(T)$ and $f(T-1)$ agree mod $T^{2n+1}(T-1)^{2n+1}$. Since these polynomials both have degree at most $2n+1$, they must be equal. □

Acknowledgments

I thank J. Lagarias for pointing out this problem, and for editorial comments and references. I also thank E. H. Brooks for introducing the author to Wolstenholme's theorem, and for helpful comments. This work was supported in part by NSF grants DMS-0943832 and DMS-1101373.

References

[1] C. Babbage, Demonstration of a theorem relating to prime numbers, *Edinburgh Philosophical J.* **1** (1819) 46–49.
[2] L. Carlitz, Note on a theorem of Glaisher, *J. London Math. Soc.* **28** (1953) 245–246.
[3] J. W. L. Glaisher, Congruences relating to the sums of products of the first n numbers and to other sums and products, *Q. J. Math.* **31** (1899) 2–35.
[4] ———, On the residues of the sums of the inverse powers of numbers in arithmetical progression, *Q. J. Math.* **32** (1900) 271–288.
[5] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic Mathematics*, CRM Proceedings & Lecture Notes, Vol. 20 (American Mathematical Society, Providence, RI, 1997), pp. 253–276.

[6] M. E. Hoffman, Quasi-symmetric functions and mod p multiple harmonic sums, preprint (2004); arXiv:math/0401319 [math.NT].

[7] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math. (2)* **39**(2) (1938) 350–360.

[8] R. Meštrović, Wolstenholme's theorem: Its generalization and extensions in the last hundred and fifty years (1862–2012), preprint (2011); arXiv:1111.3057 [math.NT].

[9] ———, On the mod p^7 determination of $\binom{2p-1}{p-1}$, preprint (2012); arXiv:1108.1174.

[10] Y. Morita, A p-adic analogue of the Γ-function, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **22**(2) (1975) 255–266.

[11] ———, A p-adic integral representation of the p-adic L-function, *J. Reine Angew. Math.* **302** (1978) 71–95.

[12] J. Rosen, Multiple harmonic sums and p-adic L-functions, preprint (2013).

[13] R. Tauraso, More congruences for central binomial coefficients, *J. Number Theory* **130**(12) (2010) 2639–2649.

[14] L. Van Hamme, Some congruences involving the p-adic gamma function and some arithmetical consequences, in *p-Adic Functional Analysis*, Lecture Notes in Pure and Applied Mathematics, Vol. 222 (Dekker, New York, 2001), pp. 133–138.

[15] E. Waring, *Meditationes Algebraic* (American Mathematical Society, Providence, RI, 1991); translated from the Latin, edited and with a foreword by Dennis Weeks; with an appendix by Franz X. Mayer, translated from the German by Weeks.

[16] L. C. Washington, p-Adic L-functions and sums of powers, *J. Number Theory* **69**(1) (1998) 50–61.

[17] J. Wolstenholme, On certain properties of prime numbers, *Quart. J. Pure Appl. Math.* **5** (1862) 35–39.

[18] J. Zhao, Wolstenholme type theorem for multiple harmonic sums, *Int. J. Number Theory* **4**(1) (2008) 73–106.

[19] ———, Mod p structure of alternating and non-alternating multiple harmonic sums, *J. Théor. Nombres Bordeaux* **23**(1) (2011) 299–308.