DIVISIBILITY PROPERTIES OF A CLASS OF BINOMIAL SUMS

MARC CHAMBERLAND AND KARL DILCHER

Abstract. We study congruence and divisibility properties of a class of combinatorial sums that involve products of powers of two binomial coefficients, and show that there is a close relationship between these sums and the theorem of Wolstenholme. We also establish congruences involving Bernoulli numbers, and finally we prove that under certain conditions the sums are divisible by all primes in specific intervals.

1. Introduction

Sums of products of binomial coefficients, more simply called *binomial sums* or *combinatorial sums*, have been of considerable interest for several centuries in various areas of mathematics, in particular in combinatorics and number theory. Many such sums can be evaluated in closed form, giving rise to *combinatorial identities*. One of the earliest combinatorial identities, now commonly known as the *Vandermonde convolution*, is

$$\sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k} = \binom{x+y}{n}, \tag{1.1}$$

where $n \geq 0$ is an integer and x, y are arbitrary real numbers. It goes back to Alexandre Vandermonde in 1772; however, it is reported in [12, p. 169] that this identity was known to Chu Shih-Chieh in China as early as 1303. For an excellent treatment of binomial sums and combinatorial identities, see [12, Ch. 5]. The books [9], [10], [15], and [24] are almost exclusively devoted to this topic, and most other books on classical or enumerative combinatorics also deal with combinatorial identities to some extent. Most known combinatorial identities are collected in the well-known general tables [11], [13], and [22]. Finally, the paper [25] treats the topic in the language, and with the methods, of hypergeometric series, and various modern aspects are discussed in [26]; this last paper also contains an extensive bibliography.

In recent decades there has been renewed interest in binomial sums, primarily as a result of R. Apery's remarkable proof, in the late 1970s, of the irrationality of $\zeta(3)$ (see, e.g., [27]) which relied on properties of the sequence

$$A(n) := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2. \tag{1.2}$$

Date: May 26, 2005.

Key words and phrases. Binomial sums, combinatorial sums, Wolstenholme's Theorem, divisibility, Bernoulli numbers, irregular primes.

The second author was supported in part by the Natural Sciences and Engineering Research Council of Canada.

The renewed interest in sums of this kind led to methods of "mechanical summation", most notably the Gosper-Zeilberger (see, e.g., [12, Sect. 5.8]) and the Wilf-Zeilberger [21] algorithms which have now been implemented in several major computer algebra systems.

It is the purpose of this paper to study a special class of binomial sums, namely

$$u_{a,b}^{\varepsilon}(n) := \sum_{k=0}^{n} (-1)^{\varepsilon k} \binom{n}{k}^a \binom{2n}{k}^b, \tag{1.3}$$

for nonnegative integers a, b, n, and $\varepsilon \in \{0, 1\}$. Clearly the choice of ε determines whether the sum is alternating or not. For certain small values of a and b the sums in (1.3) have closed forms; this will be discussed in Section 2. Our initial motivation for studying the sums in (1.3) has been the observation that the sequence

$$u_{1,1}^{1}(n) = \sum_{k=0}^{n} (-1)^k \binom{n}{k}\binom{2n}{k}, \qquad n = 0, 1, 2, \ldots, \tag{1.4}$$

displays some interesting properties, including congruences similar to the well-known theorem of Wolstenholme. This will be investigated in Section 3 in greater generality. Section 4 then deals with the question of possible converses, and in the process we consider congruences modulo powers of 2. In Sections 5 and 6 we study more detailed divisibility and congruence properties (modulo odd primes) which involve Bernoulli numbers and the concepts of irregular primes and irregular pairs.

While closed forms for the sums in (1.3) exist only for very few values of ε, a, and b, Calkin [5] proved that $u_{a,0}^{1}(2n)$ is always divisible by $\binom{2n}{n}$, with a similar result holding for $u_{0,b}^{1}(n)$. In Section 7 we extend this, in a somewhat different form, to all $u_{a,b}^{\varepsilon}(n)$ under the condition that $a + b + \varepsilon$ is even. We finish this paper with some remarks on further generalizations in Section 8.

2. Closed Forms

In this brief section we collect all the closed forms for $u_{a,b}^{\varepsilon}(n)$ that are known for various values of ε, a, and b. However, we must first explain what we mean by the term "closed form". For instance, all the sums in (1.3) can easily be rewritten as special values of suitable hypergeometric functions; obviously, this cannot be meant by "closed form". A more reasonable informal definition is given in [5, p. 17], namely "a sum of a fixed number of hypergeometric terms", which means a sum of a fixed number of products and quotients of factorials and powers depending on n. This is also consistent with de Bruijn [2, p. 72].

Here, then, is the list of known closed forms. Unless otherwise indicated, a, b, and n are nonnegative integers.

$$u_{0,0}^{0}(n) = n + 1, \qquad u_{1,0}^{0}(n) = 2^n, \tag{2.1}$$

$$u_{2,0}^{0}(n) = \binom{2n}{n}, \tag{2.2}$$

$$u_{1,1}^{0}(n) = \binom{3n}{n}, \tag{2.3}$$

$$u_{a,0}^{1}(2n+1) = 0, \tag{2.4}$$

$$u_{0,0}^{1}(2n) = 1, \qquad u_{1,0}^{1}(2n) = 0 \quad (n \geq 1), \tag{2.5}$$

$$u^1_{2,0}(2n) = (-1)^n \binom{2n}{n}, \tag{2.6}$$

$$u^1_{3,0}(2n) = (-1)^n \binom{2n}{n}\binom{3n}{n} = (-1)^n \frac{(3n)!}{n!^3}. \tag{2.7}$$

Identities (2.1) and (2.5) are trivial or follow from the basic form of the binomial formula. (2.2) comes from (1.1) with $x = y = n$, and (2.3) follows from (1.1) with $x = 2n, y = n$. (2.4) follows by symmetry, and (2.6) is a well-known formula that can be found, e.g., in [10, eq. (3.81)]. Identity (2.7) is due to Dixon and can also be found, e.g., in [10, eq. (6.6)].

In order to obtain analogous identities to (2.1), (2.2) and (2.5)–(2.7) for $a = 0$, we note that a simple symmetry consideration with (1.3) leads to the identity

$$u^\varepsilon_{0,b}(n) = \frac{1}{2}\left\{ u^\varepsilon_{b,0}(2n) + (-1)^{\varepsilon n}\binom{2n}{n}^b \right\}. \tag{2.8}$$

With this we immediately obtain

$$u^0_{0,1}(n) = 2^{2n-1} + \frac{1}{2}\binom{2n}{n}, \tag{2.9}$$

$$u^0_{0,2}(n) = \frac{1}{2}\binom{4n}{2n} + \frac{1}{2}\binom{2n}{n}^2, \tag{2.10}$$

$$u^1_{0,1}(n) = \frac{(-1)^n}{2}\binom{2n}{n} \quad (n \geq 1), \tag{2.11}$$

$$u^1_{0,2}(n) = \frac{(-1)^n}{2}\left\{ \binom{2n}{n} + \binom{2n}{n}^2 \right\}, \tag{2.12}$$

$$u^1_{0,3}(n) = \frac{(-1)^n}{2}\binom{2n}{n}\left\{ \binom{3n}{n} + \binom{2n}{n}^2 \right\}. \tag{2.13}$$

No other closed forms are known. In fact, de Bruijn [2, pp. 72 ff.] used asymptotic methods to show that no closed forms for $u^1_{a,0}(2n)$ can exist for $a \geq 4$, and it is reported in [5] that for $3 \leq a \leq 9$ there is no closed form for $u^0_{a,0}(n)$.

3. Connections with Wolstenholme's theorem

A well-known result of Wolstenholme states that for any prime $p \geq 5$ one has

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}. \tag{3.1}$$

This congruence is of interest also because no composite integer is known for which it holds, and the truth of the converse of Wolstenholme's theorem seems to be a difficult problem. For a brief history, generalizations, and references on this problem, see [19].

If we study the first terms of the sequence in (1.4), namely (starting with $n = 0$) $1, -1, -1, 8, -17, -1, 116, -334, 239, 1709, -7001, 9316, \ldots$, a congruence pattern similar to (3.1) emerges. In fact, it appears that we have $u^1_{1,1}(p) \equiv -1 \pmod{p^3}$ for all primes $p \geq 5$. This fact can be obtained in greater generality for $u^\varepsilon_{a,b}(p)$, using Wolstenholme's theorem.

Theorem 3.1. *For any prime $p \geq 5$ we have*

$$u_{a,b}^{\varepsilon}(p) \equiv 1 + (-1)^{\varepsilon} 2^b \pmod{p^3}, \tag{3.2}$$

except when $(\varepsilon, a, b) = (0, 0, 1)$ or $(0, 1, 0)$.

The proof of this result depends on the following lemma which is of interest in its own right. Let $v_{a,b}^{\varepsilon}(n)$ be the sum $u_{a,b}^{\varepsilon}(n)$ without the first and the last terms, i.e.,

$$v_{a,b}^{\epsilon}(n) := \sum_{k=1}^{n-1} (-1)^{\varepsilon k} \binom{n}{k}^a \binom{2n}{k}^b. \tag{3.3}$$

This sum will be mainly of interest when n is a prime.

Lemma 3.1. *For any odd prime p we have*

$$v_{a,b}^{\varepsilon}(p) \equiv 0 \pmod{p^{a+b+1}}, \tag{3.4}$$

except when $\varepsilon = 0$ and $a + b$ is odd, or when $\varepsilon = 0$ and $p - 1 \mid a + b$, in which cases the congruence (3.4) *holds only modulo p^{a+b}.*

Proof. For an odd prime p and $1 \leq k \leq p - 1$ we have

$$\begin{aligned} \binom{p}{k} &= p \frac{(p-1)(p-2)\cdots(p-k+1)}{k!} \\ &\equiv p \frac{(-1)(-2)\cdots(-k+1)}{k!} \equiv p \frac{(-1)^{k-1}}{k} \pmod{p^2}, \end{aligned} \tag{3.5}$$

and similarly

$$\binom{2p}{k} \equiv 2p \frac{(-1)^{k-1}}{k} \pmod{p^2}.$$

Substituting this into (3.3), we get

$$v_{a,b}^{\varepsilon}(p) \equiv (-1)^{a+b} 2^b p^{a+b} \sum_{k=1}^{p-1} \frac{(-1)^{(\varepsilon+a+b)k}}{k^{a+b}} \pmod{p^{a+b+1}}. \tag{3.6}$$

First, let $a + b \equiv \varepsilon \pmod 2$. It is a well-known fact that

$$\sum_{k=1}^{p-1} \frac{1}{k^{a+b}} \equiv 0 \pmod{p} \tag{3.7}$$

whenever $a + b$ is not a multiple of $p - 1$; see, e.g., [17, p. 353].

Next, suppose that $a + b \not\equiv \varepsilon \pmod 2$. If $a + b$ is even then we have

$$2 \sum_{k=1}^{p-1} \frac{(-1)^k}{k^{a+b}} \equiv \sum_{k=1}^{p-1} \frac{(-1)^k}{k^{a+b}} + \sum_{k=1}^{p-1} \frac{(-1)^k}{(p-k)^{a+b}} \pmod{p} \tag{3.8}$$

$$= \sum_{k=1}^{p-1} \frac{(-1)^k}{k^{a+b}} + \sum_{k=1}^{p-1} \frac{(-1)^{p-k}}{k^{a+b}} = 0 \pmod{p}, \tag{3.9}$$

since p is odd. This and (3.7), respectively, combined with (3.6), proves the lemma. □

Remark. Lemma 3.1 will be considerably improved upon in Sections 5 and 6. However, in its present form it is sufficient for the following proof.

Proof of Theorem 3.1. Using Wolstenholme's congruence (3.1), we obtain with the definitions (1.3) and (3.3),

$$\begin{aligned} u_{a,b}^{\varepsilon}(p) &= 1 + (-1)^{\varepsilon}\binom{2p}{p}^b + v_{a,b}^{\varepsilon}(p) \\ &= 1 + (-1)^{\varepsilon}2^b\binom{2p-1}{p-1}^b + v_{a,b}^{\varepsilon}(p) \\ &\equiv 1 + (-1)^{\varepsilon}2^b + v_{a,b}^{\varepsilon}(p) \pmod{p^3}. \end{aligned}$$

By Lemma 3.1 we are done, with the exception of the following special cases: $u_{1,0}^1(p) = 0$ by (2.4), while by (2.11) we have

$$u_{0,1}^1(p) = \frac{-1}{2}\binom{2p}{p} \equiv -1 \pmod{p^3}, \tag{3.10}$$

by Wolstenholme's theorem. Both cases are consistent with (3.2). Finally, when $\varepsilon = 0$ and $a = b = 1$, the only exceptional prime is $p = 3$ (see Remark (2) above), which is not covered by the theorem. This completes the proof. □

Remarks.

(1) Since (3.10) shows that this case is equivalent to Wolstenholme's theorem itself (as are the cases related to (2.2), (2.6), and (2.11)), Theorem 3.1 can be considered a generalization of Wolstenholme's theorem.

(2) While it is conjectured that the converse of Wolstenholme's theorem is true, this will not be the case for Theorem 3.1 in general. For instance, calculations show that we have $u_{1,1}^1(n) \equiv -1 \pmod{n^3}$ for the composite integers $n = 10$, 25, 146, and 586. These are all up to 1000, but there are a total of 75 such composite integers up to 10^5; all have exactly two prime divisors, one of which is always 2 or 5.

Theorem 3.1 is not valid for $p = 2$ or $p = 3$ since the proof depends on Wolstenholme's theorem which fails for these two primes. However, the sums $u_{a,b}^{\varepsilon}(p)$ have only three, resp. four terms when $p = 2$, resp. $p = 3$, so that it is easy to deal with these special cases separately. Also, since there is no reliance on Wolstenholme's theorem, it will be possible to prove the respective converses.

Theorem 3.2. *Let $\varepsilon \in \{0, 1\}$, and $a, b \geq 0$ be integers. Then*

$$u_{a,b}^{\varepsilon}(2) \equiv 1 + (-1)^{\varepsilon}2^b \pmod{8} \tag{3.11}$$

if and only if

$$\begin{cases} b \geq 2, \text{ or} \\ b = 1 \text{ and } a \geq 1, \text{ or} \\ b = 0,\ \varepsilon = 1, \text{ and } a = 1, \text{ or} \\ b = 0,\ \varepsilon = 0, \text{ and } a \geq 3. \end{cases}$$

We also have

$$u_{a,b}^{\varepsilon}(3) \equiv 1 + (-1)^{\varepsilon}2^b \pmod{27} \tag{3.12}$$

if and only if

$$\begin{cases} b \geq 3 \text{ and } 3 \mid b, \text{ or} \\ b = 1,\ \varepsilon = 0, \text{ and } a = 1, \text{ or} \\ b = 0,\ \varepsilon = 1, \text{ and } a = 2, \text{ or} \\ b = 0,\ \varepsilon = 1, \text{ and } a = 1. \end{cases}$$

Proof. From (1.3) we immediately get

$$u_{a,b}^{\varepsilon}(2) = 1 + (-1)^{\varepsilon} 2^{a+2b} + 2^b 3^b. \tag{3.13}$$

For $a + 2b \geq 3$ the second term on the right vanishes modulo 8, and for $b \geq 1$ we have $2^b 3^b \equiv (-1)^{\varepsilon} 2^b \pmod 8$. This proves (3.11) in the first two cases, while for $(a, b) = (0, 1)$ the congruence does not hold. This leaves the case $b = 0$, and we see immediately that (3.11) holds if and only if $2^a \equiv 1 - (-1)^{\varepsilon} \pmod 8$. When $\varepsilon = 1$, this is only possible for $a = 1$, while in the case $\varepsilon = 0$ the congruence holds exactly when $a \geq 3$. We have thus covered all cases for the first half of the theorem.

For the second half we use again (1.3) to obtain

$$u_{a,b}^{\varepsilon}(3) = 1 + (-1)^{\varepsilon} 3^a 6^b + 3^a 15^b + (-1)^{\varepsilon} 20^b, \tag{3.14}$$

and for $a + b \geq 3$ this reduces to

$$u_{a,b}^{\varepsilon}(3) \equiv 1 + (-1)^{\varepsilon} 20^b \pmod{27}, \tag{3.15}$$

so (3.12) holds if and only if $10^b \equiv 1 \pmod{27}$. Since $10^b = (1 + 9)^b \equiv 1 + 9b \pmod{27}$, the congruence (3.15) holds if and only if $3 \mid b$. This proves the result for $a + b \geq 3$. The few remaining pairs (a, b) are easy to check using (3.14), which leads to the last three cases; we omit the details. □

4. Exceptions to the converse of Theorem 3.1

As mentioned in the introduction to Section 3, the validity of the converse of Wolstenholme's theorem is a difficult unsolved problem. It is therefore natural to ask whether or not for each triple (ε, a, b) the converse of Theorem 3.1 holds, i.e., whether there are composite integers p for which the congruence (3.2) holds.

We already remarked at the end of Section 3 that for $(\varepsilon, a, b) = (1, 1, 1)$ counterexamples exist. Computations show that there are many more cases in which there are counterexamples to the converse of Theorem 3.1; however, all the composites for which (3.2) holds seem to be powers of 2. We shall now explain this phenomenon.

Theorem 4.1. *Let $\varepsilon \in \{0, 1\}$, $a \geq 0$, and $b \geq 4$ be integers. Then*

$$u_{a,b}^{\varepsilon}(2^r) \equiv 1 + (-1)^{\varepsilon} 2^b \pmod{2^{3r}} \tag{4.1}$$

if and only if

$$2 \leq r \leq \left\lfloor \frac{2b + 3 - (-1)^b}{6} \right\rfloor \qquad \text{for} \quad \varepsilon = 1, \tag{4.2}$$

or

$$2 \leq r \leq \left\lfloor \frac{2b + 2s + 3 + (-1)^b}{6} \right\rfloor \qquad \text{for} \quad \varepsilon = 0, \tag{4.3}$$

except when $(\varepsilon, a, b) = (0, 0, 4)$, in which case (4.1) holds for $2 \leq r \leq 3$. In addition, for $(\varepsilon, a, b) = (0, 1, 2)$ we have (4.1) with $r = 2$.

Remarks.

(1) With the exception of $(\varepsilon, a, b) = (1, 1, 1)$ and the cases covered by this result, we have not observed any other counterexamples to the converse of Theorem 3.1.

(2) Theorem 3.2 can be seen as supplementary to Theorem 4.1 for $r = 1$.

For the proof of Theorem 4.1 we need some congruences of certain binomial coefficients modulo powers of 2. Congruence (4.4) below could probably be obtained

as special case of the very general results in [14]; see also [6] for (4.6). However, for the sake of simplicity and completeness we give separate proofs.

Lemma 4.1. *Let $r \geq 1$. Then*

$$\binom{2^{r+1}-1}{2^r-1} \equiv 3 \pmod 8, \tag{4.4}$$

$$\binom{2^{r+1}}{2^r} \equiv 6 \pmod{16}, \tag{4.5}$$

$$\binom{2^{r+1}}{k} \equiv 0 \pmod 4 \qquad (1 \leq k \leq 2^r-1). \tag{4.6}$$

Proof. To prove (4.4), we rewrite

$$\binom{2^{r+1}-1}{2^r-1} = \frac{(2^{r+1}-1)(2^{r+1}-2)(2^{r+1}-3)\cdots(2^r+1)}{(2^r-1)(2^r-2)(2^r-3)\cdots 1}.$$

We see that each power of 2 in the denominator is matched with an equal power of 2 in the numerator. Thus we can eliminate all these powers of 2. Let $g(n)$ denote the integer n with all powers of 2 removed. Then we have

$$\binom{2^{r+1}-1}{2^r-1} = \frac{(2^{r+1}-1)!}{2^r(2^r-1)!^2} = \frac{g((2^{r+1}-1)!)}{g((2^r-1)!)^2} \equiv g((2^{r+1}-1)!) \pmod 8, \tag{4.7}$$

since $x^2 \equiv 1 \pmod 8$ for any odd integer x. Now

$$\begin{aligned} g((2^{r+1}-1)!) &= g((2^{r+1}-1)(2^{r+1}-2)(2^{r+1}-3)\cdots 2\cdot 1 \\ &= (2^{r+1}-1)(2^{r+1}-3)\cdots 3\cdot 1\cdot g((2^r-1)!). \end{aligned}$$

When $r \geq 2$, we have

$$(2^{r+1}-1)(2^{r+1}-3)\cdots 3\cdot 1 \equiv \big((-1)(-3)(-5)(-7)\big)^{2^{r-2}} \equiv 1 \pmod 8,$$

and thus,

$$g((2^{r+1}-1)!) \equiv g((2^r-1)!) \pmod 8. \tag{4.8}$$

For $r = 2$ we have $g((2^2-1)!) = g(6) = 3$; hence using (4.8) we get by induction, $g((2^{r+1}-1)!) \equiv 3 \pmod 8$. This, with (4.7), implies (4.4).

Next, since the left-hand side of (4.5) is twice the left-hand side of (4.4), we immediately get (4.5). Finally, we write

$$\binom{2^{r+1}}{k} = \frac{2^{r+1}}{k} \cdot \frac{(2^{r+1}-1)(2^{r+1}-2)\cdots(2^{r+1}-k+1)}{1\cdot 2\cdot 3\cdots(k-1)}, \tag{4.9}$$

and by matching factors in the numerator and denominator of the right-most fraction we see that the exact power of 2 dividing the binomial coefficient is the same as that dividing $2^{r+1}/k$. Since the highest possible power of 2 in k is 2^{r-1}, this proves (4.6). □

Remark. The congruence (4.6) can easily be refined. For instance, (4.9) shows immediately that for $r \geq 2$ the highest power of 2 dividing $\binom{2^{r+1}}{k}$ for $1 \leq k \leq 2^r-1$ is 2^2 exactly when $k = 2^{r-1}$, and it is at least 2^3 for all other k in this range.

For the next lemma and the proof of the theorem we use the notation $\mathrm{ord}_2(n)$ to mean the highest power of 2 that divides the integer n.

Lemma 4.2. (*a*) *When $b \geq 1$ is odd, then*

$$\operatorname{ord}_2(3^b - 1) = 1. \tag{4.10}$$

(*b*) *When $b = 2^s t$, $s \geq 1$ and $t \geq 1$ is odd, then*

$$\operatorname{ord}_2(3^b - 1) = s + 2. \tag{4.11}$$

Proof. (a) Since $3^c \equiv 1 \pmod 8$ for any even integer $c \geq 1$, we have $3^b \equiv 3 - 1 \pmod 8$, which implies (4.10).

(b) First we use the well-known fact (see, e.g., [20, p. 103]) that for odd integers a we have

$$a^{2^s} \equiv 1 \pmod{2^{s+2}}; \tag{4.12}$$

raising both sides to the power t shows that the order in (4.11) is at least $s + 2$. On the other hand, we show by induction that the congruence (4.12) does not hold modulo 2^{s+3} when $a = 3$. Indeed, if this were the case then factoring (4.12) would give

$$\left(3^{2^{s-1}} - 1\right)\left(3^{2^{s-1}} + 1\right) = C2^{s+3}$$

for some integer C. But $\operatorname{ord}_2(3^{2^{s-1}}+1) = 1$ for any $s \geq 2$, and thus $\operatorname{ord}_2(3^{2^{s-1}}-1) \geq s+2$. Thus, going backwards, we would obtain $\operatorname{ord}_2(3^2-1) \geq 4$, which is false. This shows that (4.12) is best possible for $a = 3$. Finally, we consider the factorization

$$3^{2^s t} - 1 = \left(3^{2^s} - 1\right)\left(3^{2^s(t-1)} + 3^{2^s(t-2)} + \ldots + 3^{2^s} + 1\right).$$

Since the right-most factor has an odd number (namely t) of odd terms, we have $\operatorname{ord}_2(3^b - 1) = \operatorname{ord}_2(3^{2^s} - 1)$, which proves (4.11). □

Proof of Theorem 4.1. By (1.3), and since n is even, we have

$$u^{\varepsilon}_{a,b}(2^r) = 1 + \binom{2^{r+1}}{2^r}^b + v^{\varepsilon}_{a,b}(2^r). \tag{4.13}$$

It is a well-known fact that $2 \mid \binom{2^r}{k}$ for $1 \leq k \leq 2^r - 1$; this is actually analogous to (4.6) and can be shown with the same arguments. This with (4.6) and (3.3) shows that

$$\operatorname{ord}_2(v^{\varepsilon}_{a,b}(2^r)) \geq 2b + a. \tag{4.14}$$

To deal with the binomial coefficient in (4.13), we note that by (4.5) there is an integer c such that

$$\binom{2^{r+1}}{2^r}^b + 2^b = 2^b(3 + 8c)^b + 2^b \equiv 2^b(3^b + 8bc3^{b-1} + 1) \pmod{2^{b+3}}.$$

Since $3^b + 1 \equiv 2$ or $4 \pmod 8$ according as b is even, resp. odd, we have

$$\operatorname{ord}_2\left(\binom{2^{r+1}}{2^r}^b + 2^b\right) = \begin{cases} b+1 & \text{if } b \text{ is even,} \\ b+2 & \text{if } b \text{ is odd.} \end{cases} \tag{4.15}$$

Next, using once again a binomial expansion, we have

$$\binom{2^{r+1}}{2^r}^b - 2^b = 2^b\left(3^b - 1 + 8bc3^{b-1} + \sum_{j=2}^{b}\binom{b}{j}8^j c^j 3^{b-j}\right). \tag{4.16}$$

Since we can write

$$\binom{b}{j}8^j = 8b\binom{b-1}{j-1}\frac{8^{j-1}}{j},$$

and for $j \geq 2$ the rational number $8^{j-1}/j$ is certainly 2-integral, i.e., the denominator is not divisible by 2, the highest power of 2 dividing the right-most sum in (4.16) has at least exponent $\mathrm{ord}_2(8b)$. Now, for $b = 2^s t$, t odd, we have $\mathrm{ord}_2(8b) = s + 3$. Hence (4.10) and (4.11) applied to (4.16) give

$$\mathrm{ord}_2\left(\binom{2^{r+1}}{2^r}^b - 2^b\right) = \begin{cases} b+s+2 & \text{if } b \text{ is even,} \\ b+1 & \text{if } b \text{ is odd.} \end{cases} \tag{4.17}$$

After these preliminaries we are ready to prove the statements of the theorem. We begin with $\varepsilon = 1$. Then with (4.13) and (4.15) we have

$$\mathrm{ord}_2(u^1_{a,b}(2^r) - 1 + 2^b) = b + \frac{3}{2} - \frac{1}{2}(-1)^b, \tag{4.18}$$

provided that the right-hand side is less than $2b + a$, by (4.14). It is easy to check that this is true for all $b \geq 2$, $a \geq 0$, and for $b = 1$, $a \geq 2$. Now it is clear that (4.1) holds if and only if the expression in (4.18) is at least $3r$; but this is equivalent to (4.2). The cases $(a, b) = (0, 1), (1, 1)$ can be excluded by checking that (4.1) does not hold for $r = 2$. Similarly, for all $b < 4$ we would get $r < 2$.

Finally, we consider $\varepsilon = 0$. Then with (4.13) and (4.17) we have

$$\mathrm{ord}_2(u^0_{a,b}(2^r) - 1 - 2^b) = b + 2 + \frac{3}{2} + \frac{1}{2}(-1)^b, \tag{4.19}$$

Once again we check that the right-hand side is less than $2b + a$; this is the case for all $b \geq 4$, $a \geq 0$, as well as for the following cases: $b = 4$ and all $a \geq 1$; $b = 3$ and all $a \geq 0$; $b = 2$ and all $a \geq 2$; $b = 1$ and all $a \geq 1$. In all these cases the congruence (4.1) holds if and only if (4.19) is at least $3r$, which is equivalent to (4.3). Also, it is easy to see that for all $b < 4$ we would once again get $r < 2$. The few cases not covered above can be checked by computation, which leads to the final statement of the theorem. □

5. Connections with Bernoulli numbers: the case $\varepsilon = 0$

In this section we study in greater detail the sums $v^{\varepsilon}_{a,b}(p)$ that were defined in (3.3). Here we assume that p is always an odd prime. In particular, we deal with the two exceptional cases of Lemma 3.1, and also improve on the congruence (3.4).

Throughout this section we make use of the *Bernoulli numbers* B_n defined by the generating function

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}, \quad |x| < 2\pi. \tag{5.1}$$

It is easy to find the values $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_4 = -1/30$, and $B_n = 0$ for all odd $n \geq 3$. Furthermore, $(-1)^{n-1}B_{2n} > 0$ for all $n \geq 1$. These and many other properties can be found, for instance, in [1], [12], [23], or [28]. A fairly complete bibliography can be found in [8].

It is clear from the proof of Lemma 3.1 that in order to deal with the exceptional cases of that result, we have to evaluate, modulo p, the sum on the right-hand side of (3.6). Congruences for non-alternating sums have been known since the late

19th century (see [17] for more details), and these can easily be used to obtain congruences for alternating sums as well.

Lemma 5.1. *Let p be an odd prime. Then for any integer m, $2 \le m < \frac{p-1}{2}$, we have*

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k^{2m-1}} \equiv \frac{2}{2m-1}\left(2^{2-2m}-1\right) B_{p+1-2m} \pmod{p}. \tag{5.2}$$

Furthermore,

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k} \equiv -2\frac{2^{p-1}-1}{p} \pmod{p}. \tag{5.3}$$

Proof. Clearly,

$$\begin{aligned}\sum_{k=1}^{p-1} \frac{(-1)^k}{k^{2m-1}} &= 2\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k)^{2m-1}} - \sum_{k=1}^{p-1} \frac{1}{k^{2m-1}} \\ &\equiv 2^{2-2m} \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^{2m-1}} \pmod{p},\end{aligned} \tag{5.4}$$

where we have used the congruence (3.7). By Fermat's little theorem, and using the congruence (17) in [17, p. 354], we get

$$\begin{aligned}\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^{2m-1}} &\equiv \sum_{k=1}^{\frac{p-1}{2}} k^{p-2m} \pmod{p} \\ &\equiv \left(1-2^{p+1-2m}\right) \frac{B_{p+1-2m}}{2^{p+1-2m}\frac{p+1-2m}{2}} \pmod{p} \\ &\equiv \left(2^{2m-2}-1\right) \frac{2}{1-2m} B_{p+1-2m} \pmod{p}.\end{aligned}$$

This, combined with (5.4), gives (5.2). The congruence (5.3) is proved in [18, p. 474]; it can also be found in [20, p. 97], Problem 14. □

Remark. The quotient in (5.3), namely

$$q_p(2) := \frac{2^{p-1}-1}{p},$$

is the well-known *Fermat quotient* to base 2. A prime p for which it vanishes modulo p is called a *Wieferich prime*. Only two such primes are known, namely $p = 1093$ and $p = 3511$; no others have been found up to 1.25×10^{15}; see [16]. Fermat quotients and Wieferich primes are also related to the classical theory of Fermat's last theorem; see, e.g., [23].

We are now ready to deal with the exceptional cases in Lemma 3.1.

Theorem 5.1. *Let p be an odd prime.*
(1) *Let $a+b$ be odd, and let $2m-1$ be the least positive remainder of $a+b$ modulo $p-1$. If $2 \le m < \frac{p-1}{2}$, then*

$$v_{a,b}^0(p) \equiv 2^{b+1} p^{a+b} \frac{1-2^{2-2m}}{2m-1} B_{p+1-2m} \pmod{p^{a+b+1}}. \tag{5.5}$$

(2) *If* $a+b \equiv 1 \pmod{p-1}$, *then*

$$v_{a,b}^0(p) \equiv 2^{b+1}p^{a+b}q_p(2) \pmod{p^{a+b+1}}. \tag{5.6}$$

(3) *If* $p-1 \mid a+b$, *then*

$$v_{a,b}^0(p) \equiv -2^b p^{a+b} \pmod{p^{a+b+1}}. \tag{5.7}$$

Proof. In all three cases we use (3.6). Then (5.2) and (5.3) immediately give (5.5) and (5.6), respectively, if we use the fact that by Fermat's little theorem we have $k^{-(a+b)} \equiv k^{-(2m-1)} \pmod{p}$.

If $p-1 \mid a+b$, then $a+b$ is even and $k^{a+b} \equiv 1 \pmod{p}$ for all $1 \le k \le p-1$, so the sum in (3.6) is congruent to $p-1 \equiv -1 \pmod{p}$, which gives (5.7). □

We restate now the most common case, namely (5.5), for small values of $a+b$.

Corollary 5.1. *Let* $p \ge 7$ *be a prime and* $a+b$ *odd with* $3 \le a+b \le p-4$. *Then*

$$v_{a,b}^0(p) \equiv p^{a+b}\frac{2^{b+1}-2^{2-a}}{a+b}B_{p-a-b} \pmod{p^{a+b+1}}. \tag{5.8}$$

Examples.

(1) From (5.8) we immediately get, for $p \ge 7$,

$$v_{2,1}^0(p) \equiv p^3 B_{p-3} \pmod{p^4}, \qquad v_{1,2}^0(p) \equiv 2p^3 B_{p-3} \pmod{p^4}.$$

(2) Let $a=b=1$ and $p=3$. Then we can easily compute

$$v_{1,1}^0(3) = 63 \equiv -18 = -2\cdot 3^2 \pmod{27},$$

which is consistent with (5.7).

It is important for our purposes to note that the denominators of the Bernoulli numbers are completely determined by the *von Staudt-Clausen theorem* (see, e.g., [28, p. 56]), while the divisibility properties of the numerators are very difficult to determine and have deep connections with, among other things, the theory of cyclotomic fields and the classical theory of Fermat's last theorem; see [23] or [28]. In this connection, an odd prime p is called *irregular* if p divides the numerator of one or more of $B_2, B_4, \dots, B_{p-3}$; otherwise p is called *regular*. If $p \mid B_{2k}$ with $2k \le p-3$, then $(p, 2k)$ is called an *irregular pair*. The first few irregular primes are 37, 59, 67, 101, 103, 131, 149, 157; these were already found in the 1840s by Kummer. All irregular pairs for $p < 12\cdot 10^6$ have been determined; see [3], [4]. K. L. Jensen proved in 1915 that there are infinitely many irregular primes. However, it is not known whether there are infinitely many regular primes, although there are strong numerical evidence and heuristic arguments to support such a conjecture; see [23, pp. 106 ff.].

With the above terminology it is clear that Corollary 5.1 implies the following.

Corollary 5.2. *Let* $p \ge 7$ *be a prime and* $a+b$ *odd with* $3 \le a+b \le p-4$. *Then* p^{a+b} *always divides* $v_{a,b}^0(p)$, *while* p^{a+b+1} *divides* $v_{a,b}^0(p)$ *if and only if* $(p, p-a-b)$ *is an irregular pair or* p *divides* $2^{a+b-1}-1$.

Examples.

(3) We can find in tables (e.g., [28, p. 410]) that $(37, 32)$ is an irregular pair. Hence we have $37^6 \mid v_{a,b}^0(37)$ for all nonnegative a, b with $a+b=5$. Similarly, the pair $(59, 44)$ is the next irregular pair which means that $59^{16} \mid v_{a,b}^0(59)$ whenever $a+b=15$.

(4) The only known primes p that divide the numerator of B_{p-3} are $p = 16\,843$ and $p = 2\,124\,679$; see [3] (no others were found in [4]). Hence by Example (1) we have $p^4 \mid v_{2,1}^0(p)$ and $p^4 \mid v_{1,2}^0(p)$ for these primes.

(5) There is a connection to both Fermat and Mersenne numbers (and primes). Since $a+b$ is odd, we can factor

$$2^{a+b-1} = \left(2^{\frac{a+b-1}{2}} + 1\right)\left(2^{\frac{a+b-1}{2}} - 1\right). \tag{5.9}$$

This means that if the Fermat number $F_n = 2^{2^n} + 1$ is a Fermat prime p, then for all a, b with $a + b = 2^{n+1} + 1$ we have that p^{a+b+1} divides $v_{a,b}^0(p)$. For instance, since $F_3 = 257$ is prime, this shows that $257^{18} \mid v_{a,b}^0(257)$ whenever $a+b = 17$. It is also clear that any factor of a (composite) Fermat number has a similar divisibility property. The factorization (5.9) shows that analogous divisibility properties also hold for Mersenne numbers $M_q := 2^q - 1$ (q prime), both when they are prime, and for factors of composite M_q.

6. Connections with Bernoulli numbers: the case $\varepsilon = 1$

Our next improvement to Lemma 3.1 deals with the case $\varepsilon = 1$. The congruence (3.4) gives rise to the question as to the behavior of $v_{a,b}^{\varepsilon}(p)$ modulo p^{a+b+2}. Where previously summation formulas modulo p were sufficient, we now need analogous congruences modulo p^2. The following lemma is closely related to congruences of Glaisher, as quoted and proved in [17].

Lemma 6.1. *Let $p \geq 5$ be a prime and $2 \leq 2m \leq p-3$. Then*

$$\sum_{k=1}^{p-1} \frac{1}{k^{2m-1}} \equiv p^2 \frac{m(1-2m)}{1+2m} B_{p-1-2m} \pmod{p^3}, \tag{6.1}$$

and

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k^{2m}} \equiv p \frac{2m}{1+2m} \left(1 - 2^{-2m}\right) B_{p-1-2m} \pmod{p^2}, \tag{6.2}$$

Proof. The congruence (6.1) can be found in [17, p. 353]. To prove (6.2), we first note that

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k^{2m}} = 2^{1-2m} \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^{2m}} - \sum_{k=1}^{p-1} \frac{1}{k^{2m}}. \tag{6.3}$$

We use the congruence

$$k^{-2m} \equiv 2k^{p-1-2m} - k^{2p-2-2m} \pmod{p^2} \tag{6.4}$$

(see, e.g., [17, p. 353]; for generalizations and further applications, see [7]), which allows us to use known congruences. First, congruence (18) in [17, p. 354] gives

$$\sum_{k=1}^{\frac{p-1}{2}} k^{p-1-2m} \equiv p\left(1 - 2^{p-2-2m}\right) \frac{B_{p-1-2m}}{2^{p-1-2m}} \pmod{p^2}.$$

This congruence is actually valid modulo p^3, but if we take it only modulo p^2 then the right-hand side simplifies since $2^{p-1} \equiv 1 \pmod{p}$. Thus,

$$\sum_{k=1}^{\frac{p-1}{2}} k^{p-1-2m} \equiv \frac{p}{2}\left(2^{2m+1}-1\right) B_{p-1-2m} \pmod{p^2}. \tag{6.5}$$

Next, the same congruence (18) in [17] gives

$$\sum_{k=1}^{\frac{p-1}{2}} k^{2p-2-2m} \equiv \frac{p}{2}\left(2^{2m+1}-1\right) B_{2p-2-2m} \pmod{p^2}. \tag{6.6}$$

We now use the well-known *Kummer congruence* which in its most basic form is

$$\frac{B_{\nu+p-1}}{\nu+p-1} \equiv \frac{B_\nu}{\nu} \pmod{p}, \qquad \nu \not\equiv 0 \pmod{p-1};$$

see, e.g., [17, p. 355], or for generalizations and a proof, see [28, p. 61]. This, combined with (6.6), gives

$$\sum_{k=1}^{\frac{p-1}{2}} k^{2p-2-2m} \equiv \frac{p}{2}\left(2^{2m+1}-1\right) \frac{2m+2}{2m+1} B_{p-1-2m} \pmod{p^2}. \tag{6.7}$$

Finally, we use another congruence form [17, p. 353], namely

$$\sum_{k=1}^{p-1} \frac{1}{k^{2m}} \equiv p\frac{2m}{2m+1} B_{p-1-2m} \pmod{p^2}.$$

This, along with (6.7), (6.5), and (6.4) substituted into (6.3) immediately gives (6.2). □

We also need the following evaluation of a certain double sum modulo p. It is of interest in its own right; we actually show more than is required.

Lemma 6.2. *Let $\alpha, \beta \in \{0,1\}$, and let m, n be integers with $1 \le m, n \le p-2$, $m+n \ne p-1$, and $m+n \equiv \alpha+\beta \pmod{2}$. Let*

$$S := \sum_{k=1}^{p-1} \frac{(-1)^{\beta k}}{k^n} \sum_{j=1}^{k-1} \frac{(-1)^{\alpha j}}{j^m}. \tag{6.8}$$

Then S has the following values modulo p: (a) If $\alpha+\beta=1$ (and thus, $m+n$ odd), then

$$S = \frac{1}{n+m}\left(1-2^{1-n-m}\right) B_{p-n-m} \pmod{p}. \tag{6.9}$$

(b) If $\alpha=\beta=1$ and both m and n are odd, then

$$S \equiv \frac{2}{nm}\left(1-2^{1-m}\right)\left(1-2^{1-n}\right) B_{p-m} B_{p-n} \pmod{p}, \tag{6.10}$$

provided that $m \ne 1$ and $n \ne 1$. If $m=1$ then the term $\frac{2}{m}\left(1-2^{1-m}\right) B_{p-m}$ must be replaced by $2q_p(2)$; similarly for n.
(c) In all other cases we have

$$S \equiv 0 \pmod{p}. \tag{6.11}$$

Proof. We begin by rewriting the double sum S in (6.8) as follows:

$$\begin{aligned} S &= \sum_{1\le j<k\le p-1} \frac{(-1)^{\beta k+\alpha j}}{k^n j^m} \\ &\equiv (-1)^{n+m+\beta+\alpha} \sum_{1\le j<k\le p-1} \frac{(-1)^{\beta(p-k)+\alpha(p-j)}}{(p-k)^n (p-j)^m} \pmod p \\ &= (-1)^{n+m+\beta+\alpha} \sum_{1\le k<j\le p-1} \frac{(-1)^{\beta k+\alpha j}}{k^n j^m}. \end{aligned}$$

If we denote this last sum by $\overline{S}$, then we have $S \equiv \overline{S} \pmod p$ since $n+m+\beta+\alpha$ is even. Hence

$$2S \equiv S + \overline{S} = \left(\sum_{k=1}^{p-1} \frac{(-1)^{\beta k}}{k^n}\right)\left(\sum_{j=1}^{p-1} \frac{(-1)^{\alpha j}}{j^m}\right) - \sum_{k=1}^{p-1} \frac{(-1)^{(\beta+\alpha)k}}{k^{n+m}} \pmod p. \tag{6.12}$$

We now distinguish between a few cases:

(1) If $\beta = 0$ or $\alpha = 0$ then by (3.7) one of the sums in parentheses in (6.12) vanishes modulo p. If $\alpha = \beta = 0$, the last sum in (6.12) also vanishes, and we have $S \equiv 0 \pmod p$. If one of α, β is 1 then $n+m$ must be odd, and the last sum in (6.12) is evaluated with the help of (5.2), which immediately gives (6.9).

(2) If $\alpha = \beta = 1$, then the last sum in (6.12) vanishes modulo p, once again by (3.7). We know that n and m must either be both even or both odd. In the former case the other two sums in (6.12) vanish by (3.8), and thus $S \equiv 0 \pmod p$. If both n and m are odd, then (5.2) gives (6.10), and (5.3) accounts for the remark following (6.10).

All cases are now covered, and thus the proof is complete. □

Remarks.

(1) Lemma 6.2 could be extended to a wider range of n and m by using Fermat's little theorem, as we did before.

(2) It is worth writing Lemma 6.2(b) explicitly in the case $m = n = 1$:

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k} \sum_{j=1}^{k-1} \frac{(-1)^j}{j} \equiv 2q_p(2)^2 \pmod p.$$

It is interesting to compare this with (5.3). Arguments similar to the above proof, using the results of this lemma, show that the corresponding *triple* sum avaluates to $\frac{-4}{3} q_p(2)^3 - \frac{1}{6} B_{p-3} \pmod p$ for $p \ge 5$.

Theorem 6.1. *Let $p \ge 5$ be a prime.*
(a) If $a+b$ is even and $2 \le a+b \le p-3$, then

$$v^1_{a,b}(p) \equiv -p^{a+b+1} \frac{b 2^b}{a+b+1} \left(1 - 2^{-a-b}\right) B_{p-1-a-b} \pmod{p^{a+b+2}}. \tag{6.13}$$

(b) If $a+b$ is odd and $1 \le a+b \le p-2$, then

$$v^1_{a,b}(p) \equiv 0 \pmod{p^{a+b+2}}. \tag{6.14}$$

Proof. The outline of the proof is like that of Lemma 3.1, but here we need to find expressions for the binomial coefficients modulo p^3. From the first line of (3.5) we obtain

$$\begin{aligned}\binom{p}{k} &\equiv \frac{p}{k!}\left((-1)^{k-1}(k-1)! + p(-1)^{k-2}(k-1)!\sum_{j=1}^{k-1}\frac{1}{j}\right) \pmod{p^3}\\ &= p\frac{(-1)^{k-1}}{k}\left(1 - p\sum_{j=1}^{k-1}\frac{1}{j}\right),\end{aligned}$$

and similarly

$$\binom{2p}{k} \equiv 2p\frac{(-1)^{k-1}}{k}\left(1 - 2p\sum_{j=1}^{k-1}\frac{1}{j}\right) \pmod{p^3}.$$

These congruences, together with (3.3), give

$$v_{a,b}^{\varepsilon} \equiv (-1)^{a+b}2^b p^{a+b}\left[S_1 - p(a+2b)S_2\right] \pmod{p^{a+b+2}}, \tag{6.15}$$

where

$$S_1 := \sum_{k=1}^{p-1}\frac{(-1)^{(\varepsilon+a+b)k}}{k^{a+b}}, \qquad S_2 := \sum_{k=1}^{p-1}\frac{(-1)^{(\varepsilon+a+b)k}}{k^{a+b}}\sum_{j=1}^{k-1}\frac{1}{j}.$$

We note that (6.15) is valid for $\varepsilon \in \{0,1\}$; however, Lemma 6.2 is applicable only when $\varepsilon = 1$. First, assume that $a+b$ is even and $\varepsilon = 1$. In this case (6.2), with $2m = a+b$, gives

$$S_1 \equiv p\frac{a+b}{a+b+1}\left(1 - 2^{-a-b}\right)B_{p-1-a-b} \pmod{p^2},$$

while from (6.9) with $n = a+b$ and $m = 1$ we get

$$S_2 \equiv \frac{1}{a+b+1}\left(1 - 2^{-a-b}\right)B_{p-1-a-b} \pmod{p}.$$

These last two congruences, substituted into (6.15), give (6.13).

Next, if $a+b$ is odd and $\varepsilon = 1$ then by (6.1) we have $S_1 \equiv 0 \pmod{p^2}$. Furthermore, since $\alpha + \beta = 0$ and $n + m = a + b + 1$ is even, we have $S_2 \equiv 0 \pmod{p}$ by (6.11). This, with (6.15), gives (6.14). □

Remark. The fact that b is a factor of the right-hand side of (6.13) is consistent with the fact that, by symmetry of the sum, $v_{a,0}^1(n) = 0$ for all $a \geq 0$ and all odd n; see also (2.4).

In analogy to Corollary 5.2, the congruence (6.13) immediately implies the following.

Corollary 6.1. *Let $p \geq 5$ be a prime and $a+b$ even with $2 \leq a+b \leq p-3$ and $b \geq 1$. Then p^{a+b+1} divides $v_{a,b}^1(p)$, and p^{a+b+2} divides $v_{a,b}^1(p)$ if and only if $(p, p-1-a-b)$ is an irregular pair or p divides $2^{a+b}-1$.*

Examples.

(1) Theorem 6.1 with $a = b = 1$ gives

$$v_{1,1}^1(p) \equiv \frac{-1}{2}p^3 B_{p-3} \pmod{p^4},$$

and we have $p^4 \mid v^1_{1,1}(p)$ for $p = 16\,843$ and $p = 2\,124\,679$; see Example 4 in Section 4.

(2) Similarly, (6.13) gives

$$v^1_{1,3}(p) \equiv \frac{-9}{2} p^5 B_{p-5} \pmod{p^6},$$

and $37^6 \mid v^1_{1,3}(37)$ since $(37, 32)$ is an irregular pair.

7. Divisibility by primes in intervals

In addition to the Wolstenholme-type congruences and divisibility properties of the shortened sums $v^\varepsilon_{a,b}(n)$, we noticed that the "full sums" $u^\varepsilon_{a,b}(n)$ themselves display some striking divisibility properties. For instance, in the special case $a = 0$ computations indicated that $\frac{1}{2}\binom{2n}{n}$ divides $u^1_{0,b}(n)$ for $b \geq 1$, consistent with (2.11) – (2.13). This had already been proved by Calkin [5] who showed that $\binom{2n}{n}$ divides $u^1_{a,0}(2n)$ for all positive a and n; by (2.8) these two statements are equivalent.

For non-alternating sums Calkin [5] proved a similar result which, however, cannot be phrased in terms of binomial coefficients.

Theorem 7.1 (Calkin)**.** *Let m and n be positive integers. If p is a prime in the interval*

$$\frac{n}{m} < p < \frac{n+1}{m} + \frac{n+1-m}{m(2ma-1)}, \tag{7.1}$$

then $p \mid u^0_{2a,0}(n)$.

In this section we shall extend Calkin's results to the general case of the sum $u^\varepsilon_{a,b}(n)$, with the only restriction that $a + b \equiv \varepsilon \pmod 2$.

Theorem 7.2. *Let $a \geq 1$, $b \geq 0$, and $\varepsilon \in \{0, 1\}$ be given, such that $a + b \equiv \varepsilon \pmod 2$. For any positive integers m and n, if p is a prime in the interval*

$$\frac{n}{m} < p < n\frac{a+2b}{m(a+2b)-1} + \frac{a+b-1}{m(a+2b)-1}, \tag{7.2}$$

then $p \mid u^\varepsilon_{a,b}(n)$.

Proof. We use the main ideas of the proof of Lemma 6 in [5]. Let $mp = n + r$, where $r > 0$. Then we have

$$\begin{aligned} \binom{n}{k} = \binom{mp-r}{k} &= \frac{(mp-r)(mp-r-1)\dots(mp-r-k+1)}{k!} \\ &\equiv \frac{(-r)(-r-1)\dots(-r-k+1)}{k!} = (-1)^k \frac{(k+1)_{(r-1)}}{(r-1)!} \pmod p, \end{aligned} \tag{7.3}$$

where we have used the *rising factorial* (or *Pochhammer symbol*) $x_{(0)} = 1$ and $x_{(r)} = x(x+1)\dots(x+r-1)$. Similarly,

$$\binom{2n}{k} \equiv (-1)^k \frac{(k+1)_{(2r-1)}}{(2r-1)!} \pmod p. \tag{7.4}$$

We substitute (7.3) and (7.4) into (1.3). Since $a + b + \varepsilon$ is even by assumption, we always have the non-alternating sum

$$u^\varepsilon_{a,b}(n) \equiv \frac{1}{(r-1)!^a (2r-1)!^b} \sum_{k=0}^{mp-r} \left((k+1)_{(r-1)}\right)^a \left((k+1)_{(2r-1)}\right)^b \pmod p. \tag{7.5}$$

Since the polynomials $x_{(0)}$, $x_{(1)}, \ldots, x_{(d)}$ form an integer basis for the space of all integer polynomials of degree at most d, there exist integers $c_0, c_1, \ldots, c_d$, where $d := (r-1)(a-1) + (2r-1)b$, such that

$$\big((k+1)_{(r-1)}\big)^{a-1} \big((k+1)_{(2r-1)}\big)^{b} = \sum_{j=0}^{d} c_j (k+r)_{(j)}. \tag{7.6}$$

Since

$$(k+1)_{(r-1)}(k+r)_{(j)} = (k+1)(k+2)\cdots(k+r+j-1) = (k+1)_{(r+j-1)},$$

we get with (7.5) and (7.6), after changing the order of summation,

$$u^{\varepsilon}_{a,b}(n) \equiv \frac{1}{(r-1)!^a (2r-1)!^b} \sum_{j=0}^{d} c_j \sum_{k=0}^{mp-r} (k+1)_{(r+j-1)} \pmod{p}. \tag{7.7}$$

Another main ingredient in this proof is the fact that the inner sum in (7.7) can be evaluated in closed form if we rewrite it as

$$\begin{aligned}(r+j-1)! \sum_{k=0}^{mp-r} \binom{k+r+j-1}{k} &= (r+j-1)! \binom{mp+j}{mp-r} \\ &= \frac{(mp+j)(mp+j-1)\cdots(mp-r+1)}{r+j},\end{aligned}$$

where we have used a known combinatorial identity that can be found, e.g., in [10, eq. (1.49)]. With (7.7) we therefore get

$$\begin{aligned}u^{\varepsilon}_{a,b}(n) \equiv{}& \frac{1}{(r-1)!^a (2r-1)!^b} \\ &\times \sum_{j=0}^{d} c_j \frac{(mp+j)(mp+j-1)\cdots(mp-r+1)}{r+j} \pmod{p}.\end{aligned} \tag{7.8}$$

Now, if we assume that $r + d < p$ and (if $b \geq 1$) $2r - 1 < p$, then $p \nmid (r-1)!$, $p \nmid (2r-1)!$, and $p \nmid r + j$ for any j, $0 \leq j \leq d$, while clearly the numerator of each summand in (7.8) is divisible by p, and thus $p \mid u^{\varepsilon}_{a,b}(n)$, as required. We now rewrite the first assumption as

$$\begin{aligned}r + d &= r(a+2b) - (a+b) + 1 = (mp-n)(a+2b) - (a+b) + 1 \\ &= mp(a+2b) - n(a+2b) - (a+b) + 1 < p.\end{aligned}$$

This holds if and only if

$$p\big(m(a+2b) - 1\big) < n(a+2b) + a + b - 1,$$

which in turn is equivalent to the right-hand inequality in (7.2), while the left-hand inequality is the same as our initial assumption $mp = n + r$.

Finally, we need to verify that $2r - 1 < p$ when $b \geq 1$. But this follows from $r + d < p$ if we can show that $r - 1 \leq d$, i.e., $r - 1 \leq (r-1)(a-1) + (2r-1)b$, which is certainly true since $a \geq 1$ and $r \geq 1$. This completes the proof. □

Remarks.

(1) If we set $b = 0$ and replace a by $2a$, it is easy to see that the inequalities (7.2) reduce to (7.1).

(2) The lengths of the intervals of primes given by (7.2) become clearer if we rewrite the inequalities as follows:

$$\frac{n}{m} < p < \frac{n}{m}\left(1 + \frac{1}{m(a+2b)-1}\right) + \frac{a+b-1}{m(a+2b)-1},$$

The largest interval and, for $a > 1$, the one containing the largest "determined" primes, occurs when $m = 1$:

$$n < p < n\left(1 + \frac{1}{a+2b-1}\right) + \frac{a+b-1}{a+2b-1}.$$

Our next result shows that the case $a = 1$ is special in that in addition to the intervals of Theorem 7.2 there is another interval of primes starting at $2n$.

Theorem 7.3. *Let $b \geq 1$ and $\varepsilon \in \{0, 1\}$ be such that $b \not\equiv \varepsilon \pmod 2$, and $n \geq 1$. If p is a prime in the interval*

$$2n < p < n\left(2 + \frac{1}{b}\right) + 1, \tag{7.9}$$

then $p \mid u^{\varepsilon}_{1,b}(n)$.

Proof. Let $p = 2n + r$, $r > 0$. As in (7.3) we have

$$\binom{2n}{k} = \binom{p-r}{k} = (-1)^k \frac{(k+1)_{(r-1)}}{(r-1)!} \pmod p. \tag{7.10}$$

Since $\varepsilon + b$ is odd, with (1.3) we get

$$u^{\varepsilon}_{1,b}(n) \equiv \frac{1}{(r-1)!^b} \sum_{k=0}^{n} (-1)^k \binom{n}{k} \left((k+1)_{(r-1)}\right)^b \pmod p.$$

Just as in (7.6) and (7.7) there are integers $c_0, c_1, \ldots, c_{b(r-1)}$ such that

$$\begin{aligned} u^{\varepsilon}_{1,b}(n) &\equiv \frac{1}{(r-1)!^b} \sum_{k=0}^{n} (-1)^k \binom{n}{k} \sum_{j=0}^{b(r-1)} c_j (k+r)_{(j)} \pmod p \\ &= \frac{1}{(r-1)!^b} \sum_{j=0}^{b(r-1)} c_j j! \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{k+r+j-1}{k+r-1} \\ &= \frac{1}{(r-1)!^b} \sum_{j=0}^{b(r-1)} c_j j! (-1)^n \binom{p-2n+j-1}{p-n-1}. \end{aligned}$$

Here we have used a binomial identity that can be found, e.g., in [10, eq. (3.48)]. The binomial coefficient in the last sum is obviously 0 whenever $j < n$, so the whole sum vanishes when $b(r-1) < n$. With $r = p - 2n$ we see that this is equivalent to $bp < n + 2nb + b$, and thus $u^{\varepsilon}_{1,b}(n) \equiv 0 \pmod p$ when (7.9) holds. This completes the proof. □

Remark. Theorems 7.2 and 7.3 are best possible in the sense that when $a + b \not\equiv \varepsilon \pmod 2$ and $a, b \geq 1$, then $u^{\varepsilon}_{a,b}(n)$ is divisible by few small primes and is sometimes a prime itself. Also, in the case $a + b \equiv \varepsilon \pmod 2$ there are few small primes other than the ones in the intervals (7.2) and (7.9) that divide $u^{\varepsilon}_{a,b}(n)$.

8. Further generalizations

An obvious generalization of the sums (1.3) would be

$$u^{\varepsilon}_{a,b,c}(n) := \sum_{k=0}^{n} (-1)^{\varepsilon k} \binom{n}{k}^a \binom{2n}{k}^b \binom{3n}{k}^c, \tag{8.1}$$

or even

$$u^{\varepsilon}_{A}(n) := \sum_{k=0}^{n} (-1)^{\varepsilon k} \binom{n}{k}^{a_1} \binom{2n}{k}^{a_2} \cdots \binom{rn}{k}^{a_r}, \tag{8.2}$$

where $A := (a_1, a_2, \ldots, a_r)$. The only closed forms we could find, other than those in Section 2, occur when $A = (1, 0, \ldots, 0, 1)$. In this case the Vandermonde convolution (1.1) (with $x = rn$ and $y = n$) gives

$$u^{0}_{A}(n) = \sum_{k=0}^{n} \binom{n}{k} \binom{rn}{k} = \binom{(r+1)n}{n}.$$

Of course this is a direct generalization of (2.3).

Calculations with (8.1) show that we can expect results similar to those obtained in Sections 3–7. This is also clear from the proofs; especially the proofs of Lemma 3.1, Theorem 6.1, and Theorem 7.2 could easily be adapted to deal with the more general sums (8.2).

References

[1] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, National Bureau of Standards, 1964.

[2] N. G. de Bruijn, *Asymptotic Methods in Analysis*, Dover Publications, New York, 1981.

[3] J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, Irregular primes and cyclotomic invariants to four million, Math. Comp. **61** (1993), 151–153.

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

[5] N. J. Calkin, *Factors of sums of powers of binomial coefficients*, Acta Arith. **86** (1998), 17–26.

[6] K. S. Davis and W. A. Webb, *Pascal's triangle modulo* 4, Fibonacci Quart. **29** (1991), 79–83.

[7] K. Dilcher, *An extension of Fermat's little theorem, and congruences for Stirling numbers*, Amer. Math. Monthly **107** (2000), 936–940.

[8] K. Dilcher, L. Skula, and I. Sh. Slavutskii, *Bernoulli Numbers. Bibliography (1713-1990)*. Queen's Papers in Pure and Applied Mathematics, 87, Queen's University, Kingston, Ont., 1991. Updated on-line version: `http://www.mathstat.dal.ca/~dilcher/bernoulli.html`.

[9] G. P. Egorychev, *Integral representation and the computation of combinatorial sums*, American Mathematical Society, Providence, R.I., 1984.

[10] H. W. Gould, *Combinatorial Identities*, revised edition, Gould Publications, Morgantown, W.Va., 1972.

[11] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 6th edition, Academic Press, New York, 2000.

[12] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd edition, Addison-Wesley Publ. Co., Reading, MA, 1994.

[13] E. R. Hansen, *A Table of Series and Products*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1975.

[14] J. G. Huard, B. K. Spearman, and K. S. Williams, *Pascal's triangle* (mod 8), Europ. J. Combinatorics **19** (1998), 45–62.

[15] J. Kaucký, *Kombinatorické identity*, VEDA, Bratislava, 1975.

[16] J. Knauer and J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **74** (2005), 1559–1563.

[17] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. **39** (1938), 350–360.
[18] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Math. Annalen **60** (1905), 471–490.
[19] R. J. McIntosh, *On the converse of Wolstenholme's theorem*, Acta Arith. **71** (1995), 381–389.
[20] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, Inc., New York, etc., 1991.
[21] M. Petkovšek, H. S. Wilf, and D. Zeilberger, $A=B$, AK Peters, Wellesley, MA, 1996.
[22] A. P. Prudnikov, Yu. A. Brychkov, and O. I. Marichev, *Integrals and Series: Elementary Functions, Vol. 1*, Gordon and Breach, New York, 1988.
[23] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.
[24] J. Riordan, *Combinatorial Identities*, John Wiley & Sons, Inc., New York, 1968.
[25] R. Roy, *Binomial identities and hypergeometric series*, Amer. Math. Monthly **94** (1987), 36–46.
[26] V. Strehl, *Binomial identities — combinatorial and algorithmic aspects*, Discrete Math. **136** (1994), 309–346.
[27] A. van der Poorten, *A proof that Euler missed... Apéry's proof of the irrationality of* $\zeta(3)$. *An informal report*, Math. Intelligencer **1** (1978/79), 195–203.
[28] L. C. Washington, *Introduction to Cyclotomic Fields*, second ed., Springer-Verlag, New York, 1997.

Department of Mathematics and Computer Science, Grinnell College, Grinnell, IA 50112, USA
E-mail address: chamberl@math.grinnell.edu

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada
E-mail address: dilcher@mathstat.dal.ca