Journal of Integer Sequences, Vol. 10 (2007),
Article 07.10.1

Congruences for a Class of Alternating Lacunary Sums of Binomial Coefficients

Karl Dilcher
Department of Mathematics and Statistics
Dalhousie University
Halifax, Nova Scotia B3H 3J5
Canada
dilcher@mathstat.dal.ca

Abstract

An 1876 theorem of Hermite, later extended by Bachmann, gives congruences modulo primes for lacunary sums over the rows of Pascal's triangle. This paper gives an analogous result for alternating sums over a certain class of rows. The proof makes use of properties of certain linear recurrences.

1 Introduction

Given the importance of binomial coefficients and combinatorial sums in many areas of mathematics, it is not surprising that divisibility properties and congruences of these combinatorial objects have been extensively studied. For instance, numerous older results can be found in Dickson's *History* [2, Ch. IX], while a more modern treatment of the subject is given by Granville [4]. One such result is the following congruence due to Hermite [6] and, in the general case, Bachmann [1, p. 46].

Theorem 1 (Hermite and Bachmann)**.** *Let p be a prime and k a positive integer. Then*

$$\sum_{0<j(p-1)<k} \binom{k}{j(p-1)} \equiv 0 \pmod{p}. \tag{1}$$

Bachmann [1, p. 53] and before him Hermite [6] used this congruence to derive recurrence relations for the integer parts of Bernoulli numbers.

It is the purpose of this paper to derive an *alternating* sum analog to a special case of (1). This also has consequences in the theory of Bernoulli numbers and polynomials. In fact, a congruence for the alternating sum in the special case where k is a multiple of $p-1$, given below as Corollary 1, is instrumental in a forthcoming study of possible multiple zeros of Bernoulli polynomials [3].

While the congruence (1) is not difficult to prove, the following main result of this paper requires considerably more effort.

Theorem 2. *Let p be an odd prime and q a positive integer. Then*

$$\sum_{j=0}^{\lfloor q/2\rfloor}\binom{q(p-1)}{2j(p-1)} \equiv \begin{cases} 1 \pmod p, & \text{if } q \text{ odd;} \\ 2 \pmod p, & \text{if } q \text{ even, } p+1 \nmid q; \\ \frac{3}{2} \pmod p, & \text{if } p+1 \mid q. \end{cases} \tag{2}$$

In order to derive the desired congruence for an alternating sum, we first note that from (1) with $k = q(p-1)$ we immediately get

$$\sum_{j=0}^{q}\binom{q(p-1)}{j(p-1)} \equiv 2 \pmod p. \tag{3}$$

Then we use the obvious identity

$$\sum_{j=0}^{q}(-1)^j\binom{q(p-1)}{j(p-1)} = -\sum_{j=0}^{q}\binom{q(p-1)}{j(p-1)} + 2\sum_{j=0}^{\lfloor \frac{q}{2}\rfloor}\binom{q(p-1)}{2j(p-1)},$$

and (2) and (3) immediately give the following

Corollary 3. *Let p be an odd prime and q a positive integer. Then*

$$\sum_{j=0}^{q}(-1)^j\binom{q(p-1)}{j(p-1)} \equiv \begin{cases} 0 \pmod p, & \text{if } q \text{ odd;} \\ 2 \pmod p, & \text{if } q \text{ even, } p+1 \nmid q; \\ 1 \pmod p, & \text{if } p+1 \mid q. \end{cases} \tag{4}$$

When q is odd, it follows by symmetry that this alternating sum vanishes; this also implies the first case in (2); the case where q is even is more difficult. The congruences (1), (2), and (4) have obvious interpretations in terms of lacunary sums of elements in certain rows of Pascal's triangle.

In order to prove Theorem 2, we first derive a number of lemmas in Section 2, followed by the proof of the theorem in Section 3.

2 Auxiliary Results

We begin by stating the following classical divisibility and congruence results for binomial coefficients; see also [4].

Lemma 4. (a) (Kummer [8]) *The exact power of the prime p which divides $\binom{n}{m}$ is given by the number of "carries" when m and $n-m$ are added in base p.*

(b) (Lucas [9]) *For all primes p and nonnegative integers n, k, a, b with $0 \le a, b < p$ we have*

$$\binom{np+a}{kp+b} \equiv \binom{n}{k}\binom{a}{b} \pmod{p}. \tag{5}$$

With these results we prove the following

Lemma 5. *Let p be an odd prime and q, j integers with $2 \le q \le 2p$ and $1 \le j \le q-1$. Then*

$$\binom{q(p-1)}{j(p-1)} \equiv \begin{cases} 0 \pmod{p}, & \text{if } q \ne p+1; \\ \binom{p-1}{j-1}^2 \pmod{p}, & \text{if } q = p+1. \end{cases} \tag{6}$$

Proof. First, let $2 \le q \le p$. Then we can write in base p,

$$(q-j)(p-1) = (q-j-1)p + (p-(q-j)), \quad j(p-1) = (j-1)p + (p-j),$$

and we see that upon adding these two numbers we have one carry in base p, and we are done by Lemma 1(a).

When $q \ge p+2$, counting the carries would be more difficult, and we use instead Lucas' result (5) in its iterated form, i.e., the result applied also to $\binom{n}{k}$. We write $q = p+1+s$ with $1 \le s \le p-1$. Then clearly

$$q(p-1) = p^2 + (s-1)p + (p-s-1). \tag{7}$$

When $1 \le j \le p$, we write $j(p-1) = (j-1)p + (p-j)$, and with (5) and (7) we get

$$\binom{q(p-1)}{j(p-1)} \equiv \binom{1}{0}\binom{s-1}{j-1}\binom{p-s-1}{p-j} \equiv 0 \pmod{p},$$

since either the second binomial coefficient on the right vanishes (when $j > s$), or the third one vanishes (when $j \le s$). Next, when $j = p+1$, we have $j(p-1) = (p-1)p + (p-1)$, and

$$\binom{q(p-1)}{(p+1)(p-1)} \equiv \binom{1}{0}\binom{s-1}{p-1}\binom{p-s-1}{p-1} \equiv 0 \pmod{p}$$

for similar reasons as above. Thirdly, when $p+2 \le j \le q-1$, we write $j = p+1+t$, $1 \le t < s$. Then in base p we have $j(p-1) = p^2 + (t-1)p + (p-t-1)$, and thus

$$\binom{q(p-1)}{j(p-1)} \equiv \binom{1}{1}\binom{s-1}{t-1}\binom{p-s-1}{p-t-1} \equiv 0 \pmod{p}$$

since the last binomial coefficient on the right vanishes. This proves (6) for $q \ne p+1$.

Finally, when $q = p+1$, we write $q(p-1) = (p-1)p + (p-1)$ and $j(p-1) = (j-1)p + (p-j)$ so that, again by (5),

$$\binom{(p+1)(p-1)}{j(p-1)} \equiv \binom{p-1}{j-1}\binom{p-1}{p-j} = \binom{p-1}{j-1}^2 \pmod{p},$$

and this completes the proof of the lemma. □

The next lemma is the central ingredient in the proof of Theorem 2. The proof uses a variant of a standard method.

Lemma 6. *Let p be an odd prime and ζ a primitive $(2p-2)$th root of unity. If we define*

$$S_p(q) := \sum_{k=1}^{2p-2} \left(1+\zeta^k\right)^{(p-1)q} \tag{8}$$

for $q = 1, 2, \ldots$, then

$$S_p(q) = (2p-2) \sum_{j=0}^{\lfloor q/2 \rfloor} \binom{q(p-1)}{2j(p-1)}. \tag{9}$$

Proof. We use the well-known fact that

$$\sum_{k=1}^{2p-2} \zeta^{mk} = \begin{cases} 0, & \text{if} \quad 2p-2 \nmid m; \\ 2p-2, & \text{if} \quad 2p-2 \mid m. \end{cases} \tag{10}$$

Now, using a binomial expansion, we get with (8),

$$\begin{aligned} S_p(q) &= \sum_{k=1}^{2p-2} \sum_{m=0}^{q(p-1)} \binom{q(p-1)}{m} \left(\zeta^k\right)^m \\ &= \sum_{m=0}^{q(p-1)} \binom{q(p-1)}{m} \sum_{k=1}^{2p-2} \zeta^{mk}. \end{aligned}$$

The result now follows from (10). □

By the theory of linear recurrence relations with constant coefficients we know from the right-hand side of (8) that for fixed p the sequence $\{S_p(q)\}$, $q = 1, 2, \ldots$, is a linear recurrence sequence of order at most $2p-2$, and that the characteristic polynomial of this sequence has $(1+\zeta^k)^{p-1}, k = 1, 2, \ldots, 2p-2$, as its roots. This motivates the following lemma.

Lemma 7. *Let p be an odd prime and $f_p(x)$ the unique monic polynomial that has the numbers $(1+\zeta^k)^{p-1}$, $k = 1, 2, \ldots, 2p-2$, as its roots. Then*

$$f_p(x) \equiv x \sum_{n=0}^{2p-3} a_n x^{2p-3-n} \pmod{p}, \tag{11}$$

where for $0 \le n \le p-2$ we have

$$a_n \equiv \begin{cases} (m+1)^2, \pmod{p} & \text{if} \quad n = 2m; \\ (m+1)(m+2), \pmod{p} & \text{if} \quad n = 2m+1, \end{cases} \tag{12}$$

and for $p-1 \le n \le 2p-3$,

$$a_n \equiv -a_{2p-3-n} \pmod{p}. \tag{13}$$

Remark. The expression in (12) can also be written more concisely as

$$a_n \equiv \left\lfloor \tfrac{n+2}{2} \right\rfloor \left\lfloor \tfrac{n+3}{2} \right\rfloor \pmod{p}.$$

The right-hand side is the shifted sequence A002620 in [10].

Proof of Lemma 4. Using the well-known fact that $(1+x)^p \equiv 1 + x^p \pmod{p}$, we have

$$(1+\zeta^j)^{p-1} = \frac{(1+\zeta^j)^p}{1+\zeta^j} \equiv \frac{1+\zeta^{jp}}{1+\zeta^j} = \frac{1+(\zeta^{p-1})^j\zeta^j}{1+\zeta^j} \pmod{p}$$

for $i \neq p-1$. Then, with $\zeta^{p-1} = -1$, we have

$$(1+\zeta^j)^{p-1} \equiv \begin{cases} 1 \pmod{p}, & \text{if } j \text{ even, } j \neq p-1; \\ 0 \pmod{p}, & \text{if } j = p-1; \\ \frac{1-\zeta^j}{1+\zeta^j} \pmod{p}, & \text{if } j \text{ odd.} \end{cases} \tag{14}$$

Hence

$$f_p(x) \equiv x(x-1)^{p-2} \sum_{j=0}^{p-2} \left(x - \frac{1-\zeta^{2j+1}}{1+\zeta^{2j+1}} \right) \pmod{p}. \tag{15}$$

First, using the expansion

$$\binom{p-2}{k} = \frac{(p-2)(p-3)\cdots(p-2-k+1)}{1\cdot 2\cdots k} \equiv (-1)^k(k+1) \pmod{p}, \tag{16}$$

which can also be found in [2, p. 272], we have

$$(x-1)^{p-2} = \sum_{k=0}^{p-2} \binom{p-2}{k} (-1)^k x^{p-2-k} \equiv \sum_{k=0}^{p-2} (k+1) x^{p-2-k} \pmod{p}. \tag{17}$$

Next, if we set

$$x_j := \frac{1-\zeta^{2j+1}}{1+\zeta^{2j+1}} \tag{18}$$

and solve for ζ^{2j+1}, we get

$$\zeta^{2j+1} = \frac{1-x_j}{1+x_j},$$

and by raising this to the $(p-1)$th power, we see that the x_j, $j = 0, 1, \ldots, p-2$, are all the roots of the polynomial equation

$$(1-x)^{p-1} = -(1+x)^{p-1},$$

since ζ is a primitive $(2p-2)$th root of unity. But since

$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p-1}{2j} x^{2j} = \frac{(1+x)^{p-1} + (1-x)^{p-1}}{2}, \tag{19}$$

we see that the expressions in (18) are exactly the zeros of the polynomials on the left of (19), and thus

$$\sum_{j=0}^{p-2}\left(x-\frac{1-\zeta^{2j+1}}{1+\zeta^{2j+1}}\right)=\sum_{j=0}^{\frac{p-1}{2}}\binom{p-1}{2j}x^{2j}\equiv\sum_{j=0}^{\frac{p-1}{2}}x^{2j}\pmod p, \tag{20}$$

where we have used the congruence $\binom{p-1}{k}\equiv(-1)^k \pmod p$, which can be obtained as in (16), or see [2, p. 272]. If we define the sequence $\{\delta_j\}$ by $\delta_j=1$ when j is even and $\delta_j=0$ when j is odd, then the product of the polynomials in (17) and (20) becomes

$$\sum_{n=0}^{2p-3}\left(\sum_{k=0}^{n}(k+1)\delta_{n-k}\right)x^{2p-3-k}=\sum_{n=0}^{2p-3}a_n x^{2p-3-n},$$

where the inner sum is not usually taken over the whole range. In fact, it is easy to see that

$$a_n=\sum_{k=0}^{n}(k+1)\delta_{n-k}\quad\text{for}\quad 0\le n\le p-2, \tag{21}$$

and

$$a_n=\sum_{k=n-p+1}^{p-2}(k+1)\delta_{n-k}\quad\text{for}\quad p-1\le n\le 2p-3. \tag{22}$$

Now, for $n\le p-2$ we get from (21),

$$\begin{aligned}a_{2m}&=\sum_{k=0}^{m}(2k+1)=(m+1)^2,\\ a_{2m+1}&=\sum_{k=1}^{m+1}2k=(m+1)(m+2),\end{aligned}$$

which is just (12). In (22) we shift the order of summation, to obtain

$$a_n=\sum_{k=0}^{2p-3-n}(k+n-p+2)\delta_{p-1-k}\equiv\sum_{k=0}^{2p-3-n}(k+n+2)\delta_k\pmod p$$

since $p-1-k\equiv k \pmod 2$. Finally we reverse the order of summation, so that

$$\begin{aligned}a_n&\equiv\sum_{k=0}^{2p-3-n}(2p-3-n-k+n+2)\delta_{(2p-3-n)-k}\\ &\equiv-\sum_{k=0}^{2p-3-n}(k+1)\delta_{(2p-3-n)-k}\pmod p.\end{aligned}$$

This, with (21), accounts for (13), which completes the proof of the lemma. □

We are now ready to prove our main result.

3 Proof of Theorem 2

In view of Lemma 3 it suffices to determine the $S_p(q), q = 1, 2, \ldots$ We first find the initial values $\pmod p$ of this sequence. By the first part of Lemma 2 we immediately get the first two parts of (2) for $q \le 2p$. By the second part of (6) we have for $q = p + 1$,

$$\begin{aligned} 2\sum_{j=0}^{\lfloor q/2\rfloor} \binom{q(p-1)}{2j(p-1)} &\equiv 4 + 2\sum_{j=1}^{\frac{p-1}{2}} \binom{p-1}{2j-1}^2 \\ &= 4 + \binom{2p-2}{p-1} - (-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \pmod p, \end{aligned} \tag{23}$$

where we have used a well-known explicit formula; see, e.g., [5, Eq. (3.74)]. For the first binomial coefficient on the right we have, by (5),

$$\binom{2p-2}{p-1} = \binom{1\cdot p + (p-2)}{0\cdot p + (p-1)} \equiv \binom{1}{0}\binom{p-2}{p-1} = 0 \pmod p,$$

and as a special case of a well-known theorem of Morley (see, e.g., [4] or [7, p. 105]) we have

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \equiv 1 \pmod p.$$

Hence with (23) we get the third part of (2) for $q = p+1$. The identity (9) now immediately gives

$$S_p(q) \equiv \begin{cases} -2 \pmod p, & \text{if } q \text{ odd;} \\ -4 \pmod p, & \text{if } q \text{ even, } p+1 \nmid q; \\ -3 \pmod p, & \text{if } p+1 \mid q; \end{cases} \tag{24}$$

for $q \le 2p$. It remains to show that (24) holds for all integers $q \ge 1$.

We are done if we can show that the sequence $\{S_p(q)\}_{q\ge 1}$, as given in (24), satisfies (for *all* q) the recurrence relation $\pmod p$ whose characteristic polynomial is given by (11); in other words, we need to show that

$$a_0 S_p(n) + a_1 S_p(n-1) + \ldots + a_{2p-3} S_p(n-2p+3) \equiv 0 \pmod p \tag{25}$$

for all $n \ge 2p-2$, with the a_j as given in Lemma 4. We may obviously consider the sequence $\{-S_p(q)\}$, and since by (13) the coefficients $a_0, a_1, \ldots, a_{2p-3}$ add up to $0 \pmod p$, we may subtract a fixed constant from all terms. Hence for a fixed prime $p \ge 3$ we are done if we can show that

$$a_0 u_n + a_1 u_{n-1} + \ldots + a_{2p-3} u_{n-2p+3} \equiv 0 \pmod p \tag{26}$$

for all $n \ge 2p-2$, where

$$u_q = -S_p(q) - 3 = \begin{cases} -1, & \text{if } q \text{ odd;} \\ 1, & \text{if } q \text{ even, } p+1 \nmid q; \\ 0, & \text{if } p+1 \mid q. \end{cases}$$

This means that $\{u_q\}_{q\geq 1}$ is the alternating sequence $(-1)^q$, with 1 subtracted whenever $p+1 \mid q$. This is the motivation for computing the alternating sum of all the a_j, which by (13) is

$$\begin{aligned} 2\sum_{n=0}^{p-2}(-1)^n a_n &= 2\sum_{m=0}^{\frac{p-3}{2}}(a_{2m}-a_{2m+1}) = 2\sum_{m=0}^{\frac{p-3}{2}}\big((m+1)^2-(m+1)(m+2)\big) \\ &= -2\sum_{m=1}^{\frac{p-1}{2}} m = -\frac{(p-1)(p+1)}{4}, \end{aligned}$$

so that

$$\sum_{n=0}^{2p-3}(-1)^n a_n \equiv \frac{1}{4} \pmod p. \tag{27}$$

Now, if n is between $k(p+1)$ (for some k) and $k(p+1)+p-4$, then in the finite sequence of indices $n-2p+3, n-2p+4, \ldots, n-1, n$, there are exactly two multiples of $p+1$.

First, if $n = k(p+1)+j$ is even, with $0 \leq j \leq p-4$, then we have to subtract $a_j + a_{p+1+j}$ from (27) since u_n and u_{n-p-1} are 0 instead of 1. Since n is even, j is also even, say $j=2m$, and so by (12) we have $a_j \equiv (m+1)^2 \pmod p$, while by (13) and (12),

$$\begin{aligned} a_{p+1+j} \equiv -a_{p-4-j} &\equiv -\left(\frac{p-5-2m}{2}+1\right)\left(\frac{p-5-2m}{2}+2\right) \\ &\equiv -\big((m+1)+\tfrac{1}{2}\big)\big((m+1)-\tfrac{1}{2}\big) \\ &= -(m+1)^2+\tfrac{1}{4} \equiv -a_j+\tfrac{1}{4} \pmod p, \end{aligned}$$

so that by (27) we have

$$\sum_{n=0}^{2p-3}(-1)^n a_n - a_j - a_{p+1+j} \equiv 0 \pmod p. \tag{28}$$

Second, if n is odd, we have to add $a_j + a_{p+1+j}$ to (27) since u_n and u_{n-p-1} are 0 instead of -1. Since n is odd, so is j, say $j=2m+1$, and so by (12) we have $a_j \equiv (m+1)(m+2) \pmod p$, while by (13) and (12),

$$a_{p+1+j} \equiv -a_{p-4-j} \equiv -\left(\frac{p-5-2m}{2}+1\right)^2 \equiv -\big(m+\tfrac{3}{2}\big)^2 \pmod p,$$

so that

$$a_j + a_{p+1+j} \equiv -\tfrac{1}{4} \pmod p,$$

and thus with (27) we have

$$\sum_{n=0}^{2p-3}(-1)^n a_n + a_j + a_{p+1+j} \equiv 0 \pmod p.$$

This, together with (28), means that (26) holds for $n = k(p+1)+j$, $0 \leq j \leq p-4$.

It remains to consider the case $p-3 \le j \le p$; in this case there is only one multiple of $p+1$ among the indices $n-2p+3, \ldots, n-1, n$, and we have to add or subtract a_j, $p-3 \le j \le p$, to, resp. from (27). Due to the ranges for which (12) and (13) are valid, all four cases need to be considered separately, namely

$$\begin{aligned} a_{p-3} &\equiv \left(\frac{p-3}{2}+1\right)^2 \equiv \tfrac{1}{4} \pmod p, \\ a_{p-2} &\equiv \left(\frac{p-3}{2}+1\right)\left(\frac{p-3}{2}+2\right) \equiv -\tfrac{1}{4} \pmod p, \\ a_{p-1} &\equiv -a_{p-2} \equiv \tfrac{1}{4} \pmod p, \\ a_p &\equiv -a_{p-3} \equiv -\tfrac{1}{4} \pmod p. \end{aligned}$$

Now with (27) we obtain

$$\sum_{n=0}^{2p-3} (-1)^n a_n \pm a_j \equiv 0 \pmod p.$$

where the sign is chosen according to the parity of j, just as in the previous case.

Altogether, we have shown that the recurrence relation (26) is always satisfied, and this completes the proof.

References

[1] P. Bachmann, *Niedere Zahlentheorie. Zweiter Teil*. B. G. Teubner, Leipzig, 1910. Reprinted as two volumes in one, Chelsea, 1968.

[2] L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea, 1919.

[3] K. Dilcher, On multiple zeros of Bernoulli polynomials, preprint, 2007.

[4] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. *Organic Mathematics* (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

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

[6] Ch. Hermite, Extrait d'une lettre à M. Borchardt, *J. Reine Angew. Math.* **81** (1876), 93–95.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., Oxford University Press, 1979.

[8] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93–146.

[9] E. Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier, *Bull. Soc. Math. France* **6** (1878), 49–54.

[10] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at `http://www.research.att.com/~njas/sequences/`.

2000 *Mathematics Subject Classification*: Primary 11A07; Secondary 05A19, 11B65.

Keywords: Binomial sums, binomial coefficients, congruences.

(Concerned with sequences A002620 and A007318.)

Received September 22 2007; revised version received October 4 2007. Published in *Journal of Integer Sequences*, October 5 2007.

Return to Journal of Integer Sequences home page.