A BINOMIAL SUM RELATED TO WOLSTENHOLME'S THEOREM

MARC CHAMBERLAND AND KARL DILCHER

ABSTRACT. A certain alternating sum $u(n)$ of $n+1$ products of two binomial coefficients has a property similar to Wolstenholme's theorem, namely $u(p) \equiv -1 \pmod{p^3}$ for all primes $p \geq 5$. However, this congruence also holds for certain composite integers p which appear to always have exactly two prime divisors, one of which is always 2 or 5. This phenomenon will be partly explained and the composites in question will be characterized. We also study the sequence $u(n)$ in greater detail, especially its growth and its sign distribution.

1. INTRODUCTION

The well-known theorem of Wolstenholme states that for any prime $p \geq 5$ we have

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}. \tag{1.1}$$

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 [20]; further recent results can be found in [11].

In a recent paper [4] we studied a class of binomial sums, namely

$$u_{a,b}^{\varepsilon}(n) := \sum_{k=0}^{n} (-1)^{\varepsilon k} \binom{n}{k}^a \binom{2n}{k}^b, \tag{1.2}$$

for nonnegative integers a, b, n, and $\varepsilon \in \{0, 1\}$, and we showed that these sums are closely related to Wolstenholme's theorem:

For any prime $p \geq 5$ we have

$$u_{a,b}^{\varepsilon}(p) \equiv 1 + (-1)^{\varepsilon} 2^b \pmod{p^3}, \tag{1.3}$$

except when $(\varepsilon, a, b) = (0, 0, 1)$ or $(0, 1, 0)$; see [4, Theorem 3.1].

As in the case of Wolstenholme's theorem, this last result raises the question of a possible converse. Computations show that (1.3) holds for certain composite integers p, but we observed this only in the following two cases:

1. For many triples (ε, a, b) the congruence (1.3) holds for powers of 2, i.e., for $p = 2^r, r \geq 2$. This case has been completely characterized in [4, Theorem 4.1].

Date: April 18, 2009.

Key words and phrases. Binomial sums, binomial coefficients, Wolstenholme's Theorem, congruences, Wilf-Zeilberger method.

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

2. In the case $(\varepsilon, a, b) = (1, 1, 1)$ we observed that the congruence (1.3) holds for the composite integers $n = 10$, 25, 146, and 586. These are the only composites less than 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; see Table 1 below.

It is the purpose of this paper to (partly) explain this phenomenon. In the process we study the sums in (1.2) for $(\varepsilon, a, b) = (1, 1, 1)$ in greater details than was done in [4]. To simplify notation, we set

$$u(n) := \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{2n}{k}; \tag{1.4}$$

the first few values, for $n = 1, 2, \ldots$, are $-1, -1, 8, -17, -1, 116, -334, 239, 1709, -7001$; see also Table 3 below. The general case (1.3) for the analogue of Wolstenholme's theorem simplifies to

$$u(p) \equiv -1 \pmod{p^3}, \tag{1.5}$$

for primes $p \geq 5$. Therefore we need to study congruences for $u(n)$ modulo p^3; this will be done in Section 2, along with some congruences modulo p. In Section 3 we make some general remarks about composite solutions of (1.5), and this is followed in Section 4 by a detailed study of a special case. In Section 5 we study the sign pattern and growth behavior of the sequence $u(n)$, along with some remarks on numerical computations. We close this paper by stating a number of open problems.

2. Congruences for $u(n)$

Although no closed form for the sum in (1.4) is known (for a more general discussion on this, see [4]), the sequence $u(n)$ does in many ways behave like a sequence of binomial coefficients. One such instance is (1.5) which we already compared with (1.1). In this section we shall carry the analogy further, thus obtaining congruences that will be important for the following sections.

Wolstenholme's congruence (1.1) can be slightly rewritten as $\binom{2p}{p} \equiv 2 = \binom{2}{1} \pmod{p^3}$, and this has been generalized to

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3} \tag{2.1}$$

for all primes $p \geq 5$ and nonnegative integers m and n. According to [9], the congruence (2.1) was first obtained by Ljunggren [3]; for more recent proofs and generalizations, see [6], [9] and [11]. The following main result of this section can be seen as a one-parameter analogue to (2.1).

Theorem 2.1. *For all primes $p \geq 5$ and integers $m \geq 1$ we have*

$$u(mp) \equiv u(m) \pmod{p^3}. \tag{2.2}$$

There are numerous useful and often remarkable congruences and divisibility results for binomial coefficients; see [7, Ch. XI] for older results and [9] for a modern perspective. The following classical results will be needed in the proof of Theorem 2.1; see [9, p. 254].

Lemma 2.1. (a) (Kummer [16]) *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) (Anton [2]) *Let p^l be the exact power of p dividing $\binom{n}{m}$. Then we have*

$$\frac{(-1)^l}{p^l}\binom{n}{m} \equiv \frac{n_0!}{m_0!r_0!}\frac{n_1!}{m_1!r_1!}\cdots\frac{n_d!}{m_d!r_d!} \pmod{p}, \tag{2.3}$$

where $n = n_0 + n_1p + \ldots + n_dp^d, m = m_0 + m_1p + \ldots + m_dp^d$, and $n - m = r_0 + r_1p + \ldots + r_dp^d$, with $0 \le n_j, m_j, r_j \le p-1$.

Proof of Theorem 2.1. We split the sum in (1.4) as follows:

$$u(pm) = \sum_{k=0}^{m-1}\sum_{j=1}^{p-1}(-1)^{pk+j}\binom{pm}{pk+j}\binom{2pm}{pk+j} + \sum_{k=0}^{m}(-1)^{pk}\binom{pm}{pk}\binom{2pm}{pk}. \tag{2.4}$$

We first consider the inner sum on the right of (2.4). If we write $pm-(pk+j) = p(m-k-1)+(p-j)$, we see that in adding $pk+j$ and $pm-(pk+j)$ in base p we have at least one carry from the p^0 column to the p^1 column, and this holds for all $k = 0, 1, \ldots, m-1$. If there is another carry, it is independent of j; the same is true for $\binom{2pm}{pk+j}$. Hence, by Lemma 2.1(a) the two binomial coefficients in the sum in question are both divisible at least by p. If one of them is also divisible by p^2, we are done since then the entire inner sum is divisible by p^3, for a given k.

We are therefore left with the case where both binomial coefficients are divisible by p but not by p^2. To deal with this case, we write $m = m_0 + m_1p + \ldots + m_dp^d$, $k = k_0 + k_1p + \ldots + k_dp^d$, and $m-k-1 = r_0 + r_1p + \ldots + r_dp^d$. Then we have

$$\begin{aligned} pm &= 0 + m_0p + \ldots + m_dp^{d+1}, \\ pk+j &= j + k_0p + \ldots + k_dp^{d+1}, \\ pm-(pk+j) &= (p-j) + r_0p + \ldots + r_dp^{d+1}, \end{aligned}$$

and thus, by (2.3),

$$\frac{-1}{p}\binom{pm}{pk+j} \equiv \frac{0!}{j!(p-j)!}\frac{m_0!}{k_0!r_0!}\cdots\frac{m_d!}{k_d!r_d!} = \frac{1}{j!(p-j)!}A_k \pmod{p},$$

and similarly,

$$\frac{-1}{p}\binom{2pm}{pk+j} \equiv \frac{1}{j!(p-j)!}B_k \pmod{p},$$

where A_k, B_k depend on k (and, of course, on p and m), but not on j since m_i, k_i and r_i are independent of j. Hence we have

$$\frac{1}{p^2}\sum_{j=1}^{p-1}(-1)^j\binom{pm}{pk+j}\binom{2pm}{pk+j} \equiv A_kB_k\sum_{j=1}^{p-1}\frac{(-1)^j}{(j!(p-j)!)^2} \pmod{p},$$

but since p is odd, the right-hand sum vanishes by symmetry, and we have for all $0 \le k \le m-1$,

$$\sum_{j=1}^{p-1}(-1)^j\binom{pm}{pk+j}\binom{2pm}{pk+j} \equiv 0 \pmod{p^3}. \tag{2.5}$$

Finally we consider the last sum in (2.4). Using (2.1) and the fact that p is odd, we get

$$\sum_{k=0}^{m}(-1)^{pk}\binom{pm}{pk}\binom{2pm}{pk} \equiv \sum_{k=0}^{m}(-1)^k\binom{m}{k}\binom{2m}{k} = u(m) \pmod{p^3}.$$

This and (2.5) substituted into (2.4) give (2.2), which completes the proof. □

Another well-known congruence for binomial coefficients (in fact better known and more widely used than (2.1) and Lemma 2.1) is Lucas' Theorem which states that

$$\binom{np+a}{kp+b} \equiv \binom{n}{k}\binom{a}{b} \pmod{p} \tag{2.6}$$

for all primes p and nonnegative integers n, k, a, b with $0 \le a, b < p$; see [6] or [9], or the original paper [17].

The following congruence for the numbers $u(n)$ can be seen as an analogue of Lucas' Theorem.

Theorem 2.2. *Let $p \ge 3$ be a prime, and $m \ge 1$ and a be integers with $0 \le a \le \frac{p-1}{2}$. Then*

$$u(mp+a) \equiv u(m)u(a) \pmod{p}. \tag{2.7}$$

Proof. Using the definition (1.4) and the congruence (2.6), we get

$$\begin{aligned} u(pm+a) &= \sum_{k=0}^{m}\sum_{j=0}^{p-1}(-1)^{pk+j}\binom{pm+a}{pk+j}\binom{2pm+2a}{pk+j} \\ &\equiv \sum_{k=0}^{m}(-1)^{pk}\binom{m}{k}\binom{2m}{k}\sum_{j=0}^{p-1}(-1)^{j}\binom{a}{j}\binom{2a}{j} \pmod{p} \\ &= u(a)\sum_{k=0}^{m}(-1)^{k}\binom{m}{k}\binom{2m}{k}, \end{aligned}$$

and this gives (2.7). Here we have used the fact that $2a \le p-1$ and that p is odd. □

Lucas' Theorem (2.6) is often quoted in the form

$$\binom{n}{k} \equiv \binom{n_d}{k_d}\cdots\binom{n_1}{k_1}\binom{n_0}{k_0} \pmod{p}, \tag{2.8}$$

where n and k have the base p representations $n = n_d p^d + \cdots + n_1 p + n_0$ and $k = k_d p^d + \cdots + k_1 p + k_0$, $0 \le n_j, k_j < p$. The following partial analogue follows immediately from Theorem 2.2.

Corollary 2.1. *If the integer n is such that $n = n_d p^d + \cdots + n_1 p + n_0$ with $0 \le n_j \le \frac{p-1}{2}$ for all $j = 0, 1, \ldots, d$, then*

$$u(n) \equiv u(n_d)\cdots u(n_1)u(n_0) \pmod{p}. \tag{2.9}$$

The restriction $0 \le a \le \frac{p-1}{2}$ in Theorem 2.2 leads to the question whether there is a congruence analogous to (2.7) for the "upper half" of the range of a. This will be addressed in the following result.

Theorem 2.3. *For each integer $b \ge 1$ there is an integer $w(b)$ such that*

$$u(p-b) \equiv 2^{2-3b}w(b) \pmod{p} \tag{2.10}$$

for all primes $p \ge 2b+1$. More generally, if $m \ge 1$ is another integer, then

$$u(mp-b) \equiv 2^{2-3b}w(m)w(b) \pmod{p}, \tag{2.11}$$

again for all $p \geq 2b+1$. The sequence of integers $w(b)$ is given by

$$w(b) = \sum_{k=0}^{b-1} (-1)^k \binom{2b-1}{k} \binom{b-1}{k}. \tag{2.12}$$

Remark. Note the similarity between the sum $w(b)$ and our sum $u(n)$ defined in (1.4). Using an explicit formula for the Jacobi polynomial $P_n^{(a,b)}(x)$ (see, e.g., Eq. (3.131) in [10, p. 37] or Eq. (22.3.1) in [1, p. 775]), we have

$$w(b) = 2^{b-1} P_{b-1}^{(0,b)}(0). \tag{2.13}$$

This fact will be used in the following proof. The first few values of $w(b)$ are as follows:

b	1	2	3	4	5	6	7	8	9	10	11	12	13
$w(b)$	1	-2	1	8	-29	34	92	-512	919	818	-9151	22472	-2924

Proof of Theorem 2.3. (i) Lucas' Theorem (2.6) gives for $2b \leq p-1$,

$$\binom{mp-b}{kp+j} = \binom{(m-1)p+(p-b)}{kp+j} \equiv \binom{m-1}{k}\binom{p-b}{j} \pmod{p},$$
$$\binom{2mp-2b}{kp+j} = \binom{(2m-1)p+(p-2b)}{kp+j} \equiv \binom{2m-1}{k}\binom{p-2b}{j} \pmod{p}.$$

Using these congruences and proceeding as in the proof of Theorem 2.2 we get

$$\begin{aligned} u(mp-b) &= \sum_{k=0}^{m-1}\sum_{j=0}^{p-1} (-1)^{pk+j} \binom{mp-b}{kp+j}\binom{2mp-2b}{kp+j} \\ &\equiv \sum_{k=0}^{m-1} (-1)^k \binom{m-1}{k}\binom{2m-1}{k} \sum_{j=0}^{p-1} (-1)^j \binom{p-b}{j}\binom{p-2b}{j} \pmod{p}, \end{aligned}$$

where we have used the fact that p is odd. Next note that, again by (2.6), since $p \geq 2b+1$ we have

$$\binom{2p-2b}{j} \equiv \binom{p+(p-2b)}{j} \equiv \binom{p-2b}{j} \pmod{p}, \tag{2.14}$$

so that the right-most sum in the last formula is congruent to $u(p-b)$ modulo p, for $1 \leq b \leq \frac{p-1}{2}$. Hence by (2.12), $u(mp-b) \equiv w(m)u(p-b) \pmod{p}$, and (2.11) follows from (2.10).

(ii) To prove (2.10), we begin by rewriting the binomial coefficient

$$\begin{aligned} \binom{p-b}{j} &= \frac{(p-b)(p-b-1)\cdots(p-b-j+1)}{j!} \\ &\equiv (-1)^j \frac{b(b+1)\cdots(b+j-1)}{j!} \pmod{p} \\ &= (-1)^j \binom{j+b-1}{j} = (-1)^j \binom{j+b-1}{b-1}, \end{aligned} \tag{2.15}$$

so that we get with (2.14),

$$u(p-b) \equiv \frac{1}{(b-1)!}\sum_{j=0}^{p-2b}\binom{p-2b}{j}(j+b-1)\cdots(j+1) \pmod p. \tag{2.16}$$

To evaluate this last sum, we define the polynomial

$$f(x) := \sum_{j=0}^{p-2b}\binom{p-2b}{j}x^{j+b-1} = x^{b-1}(x+1)^{p-2b},$$

and we see that the sum in (2.16) is the $(b-1)$th derivative of f, evaluated at $x=1$. Using Leibniz's rule for higher derivatives of a product, along with the easy facts

$$\frac{d^j}{dx^j}x^{b-1}\bigg|_{x=1} = \frac{(b-1)!}{(b-j-1)!}$$

and

$$\frac{d^{b-1-j}}{dx^{b-1-j}}(x+1)^{p-2b}\bigg|_{x=1} = \frac{(p-2b)!}{(p-3b+j+1)!}2^{p-3b+j+1},$$

we obtain the expression

$$\begin{aligned} f^{(b-1)}(1) &= \sum_{j=0}^{b-1}\binom{b-1}{j}\frac{(b-1)!}{(b-j-1)!}\frac{(p-2b)!}{(p-3b+j+1)!}2^{p-3b+j+1} \\ &= 2^{p-3b+1}(b-1)!\sum_{j=0}^{b-1}\binom{b-1}{j}\binom{p-2b}{b-1-j}2^j. \end{aligned}$$

By Fermat's Little Theorem we have $2^p \equiv 2 \pmod p$, and thus by changing the order of summation we get with (2.16),

$$\begin{aligned} u(p-b) = \frac{f^{(b-1)}(1)}{(b-1)!} &\equiv 2^{2-3b}\sum_{j=0}^{b-1}\binom{b-1}{j}\binom{p-2b}{b-1-j}2^j \\ &\equiv 2^{2-3b}\sum_{j=0}^{b-1}\binom{b-1}{b-1-j}\binom{p-2b}{j}2^{b-1-j} \\ &\equiv 2^{2-3b}\sum_{j=0}^{b-1}\binom{b-1}{j}\binom{p-2b}{j}2^{b-1-j} \pmod p. \end{aligned} \tag{2.17}$$

Finally, using the same method as in (2.15), we have

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

and the sum in (2.17) (excluding the factor 2^{2-3b}) becomes, modulo p,

$$2^{b-1}\sum_{j=0}^{b-1}(-1)^j\binom{b-1}{j}\binom{2b-1+j}{j}\frac{1}{2^j} = 2^{b-1}P_{b-1}^{(0,b)}(0),$$

where the right-hand term is obtained by comparing the left-hand sum with a second explicit expression for the Jacobi polynomials; see, e.g., Equation (22.3.2) in [1, p. 775]. This, together with (2.17) and (2.13), proves (2.10), and we are done. □

As an easy consequence we get the following extension of Theorem 2.2.

Corollary 2.2. *Let $p \geq 3$ be a prime and m, a positive integers with $\frac{p+1}{2} \leq a \leq p-1$. Then*

$$u(mp+a) \equiv w(m+1)u(a) \pmod{p}. \tag{2.18}$$

In particular, we have for all $0 \leq a \leq p-1$,

$$u(3p+a) \equiv u(3)u(a) \pmod{p}. \tag{2.19}$$

Proof. Since $b := p - a$ satisfies the conditions of Theorem 2.3, using (2.11) and then (2.10) in the form $w(p-a) \equiv 2^{3(p-a)-2}u(a) \pmod{p}$, we obtain

$$\begin{aligned} u(mp+a) &= u((m+1)p - (p-a)) \\ &\equiv w(m+1)2^{2-3(p-a)}w(p-a) \pmod{p} \\ &\equiv w(m+1)u(a) \pmod{p}. \end{aligned}$$

Since $w(4) = 8 = u(3)$, we get (2.19) from (2.18) and (2.7). □

Remark. Congruences of the type (2.8) and (2.9) have been studied in a more general setting by McIntosh [19]

3. Composite solutions of (1.5)

As mentioned in the introduction, it is one of the purposes of this paper to study counterexamples to the converse of the "Wolstenholme analogue" given by the congruence (1.5), i.e., we wish to study those composite integers n for which

$$u(n) \equiv -1 \pmod{n^3} \tag{3.1}$$

holds. A numerical search for $n \leq 4 \cdot 10^6$ showed that the only composite solutions of (3.1) have exactly two prime divisors, one of which is always 2 or 5; see Table 1. For some remarks on the computations, see the final section.

n	factored	n	factored	n	factored	n	factored
10	$2 \cdot 5$	4258	$2 \cdot 2129$	10378	$2 \cdot 5189$	20546	$2 \cdot 10273$
25	5^2	5186	$2 \cdot 2593$	10786	$2 \cdot 5393$	20642	$2 \cdot 10321$
146	$2 \cdot 73$	7745	$5 \cdot 1549$	10826	$2 \cdot 5413$	20738	$2 \cdot 10369$
586	$2 \cdot 293$	8258	$2 \cdot 4129$	10834	$2 \cdot 5417$	32834	$2 \cdot 16417$
2186	$2 \cdot 1093$	8354	$2 \cdot 4177$	10898	$2 \cdot 5449$	32906	$2 \cdot 16453$
2386	$2 \cdot 1193$	8458	$2 \cdot 4229$	16418	$2 \cdot 8209$	33322	$2 \cdot 16661$
2594	$2 \cdot 1297$	8714	$2 \cdot 4357$	16546	$2 \cdot 8273$	33505	$5 \cdot 6701$
2642	$2 \cdot 1321$	8746	$2 \cdot 4373$	16706	$2 \cdot 8353$	33802	$2 \cdot 16901$
4162	$2 \cdot 2081$	8842	$2 \cdot 4421$	17026	$2 \cdot 8513$	34058	$2 \cdot 17029$
4226	$2 \cdot 2113$	10306	$2 \cdot 5153$	17674	$2 \cdot 8837$	35338	$2 \cdot 17669$

Table 1: The first 40 composite solutions to (3.1)

It is not surprising that the factors 2 and 5 should play a special role in the numerical results. In fact, in addition to $u(1)$, only $u(2)$ and $u(5)$ are equal to -1, at least up to $4 \cdot 10^6$. Since Theorem 2.1 gives, for primes $p \geq 5$,

$$u(2p) \equiv u(2) = -1 \pmod{p^3},$$

the Chinese Remainder Theorem implies that the congruence (3.1) holds for $n = 2p$ if and only if we have

$$u(2p) \equiv -1 \pmod 8. \tag{3.2}$$

Similarly we have, again by Theorem 2.1,

$$u(5p) \equiv u(5) = -1 \pmod{p^3},$$

and by the Chinese Remainder Theorem we see that (3.1) holds for $n = 5p$ if and only if $u(5p) \equiv -1 \pmod{5^3}$, which by Theorem 2.1 can be reduced to

$$u(p) \equiv -1 \pmod{125}. \tag{3.3}$$

While in the next section we are able to completely characterize the primes p satisfying the congruences (3.2), the case of (3.3) remains unsolved; see Section 6 for some further remarks.

4. The case $u(2p)$

In order to characterize the solutions of the congruence (3.2), we will first reduce it to a congruence involving a single binomial coefficient. Although only congruences modulo 8 are required, we prove slightly more.

Lemma 4.1. *For any integer $m \geq 1$ we have*

$$u(2m) \equiv \binom{6m}{2m} \pmod{16}, \tag{4.1}$$

and when m is odd,

$$u(m) \equiv \binom{3m}{m} \pmod 4. \tag{4.2}$$

Proof. For odd positive integers $k < 2m$, consider

$$\binom{2m}{k} = \frac{2m}{k}\binom{2m-1}{k-1}, \qquad \binom{4m}{k} = \frac{4m}{k}\binom{4m-1}{k-1}.$$

We see that the first expression is always even, and the second one is always divisible by 4. Hence we have

$$2\binom{2m}{k}\binom{4m}{k} \equiv 0 \pmod{16}, \qquad k = 1, 3, \ldots, 2m-1, \tag{4.3}$$

and if we add all these terms to the sum in (1.4) with $n = 2m$, we obtain

$$u(2m) \equiv \sum_{k=0}^{2m} \binom{2m}{k}\binom{4m}{k} \pmod{16}. \tag{4.4}$$

Now the right-hand side of (4.4) has the closed form expression $\binom{6m}{2m}$, which is a special case of the Vandermonde convolution; see, e.g., [10, p. 22]. This completes the proof of (4.1). The proof of (4.2) is identical with the exception that in (4.3) we have divisibility only by 4. □

Combining (4.1) and (3.2), we therefore need to know for which integers $m \geq 1$ (not necessarily prime at this point) we have

$$\binom{6m}{2m} \equiv -1 \pmod 8. \tag{4.5}$$

We begin with a lemma. For the remainder of this section, let $(m)_2$ denote the binary representation of m, written from right to left; e.g., $(20)_2 = \texttt{10100}$.

Lemma 4.2. (*a*) *The binomial coefficient* $\binom{3m}{m}$ *is odd if and only if the binary expansion of* m *has no two consecutive* `1`*s.*

(*b*) *If* $\binom{3m}{m}$ *is even, then it is divisible by 4.*

Proof. Suppose that $(m)_2$ has no two consecutive `1`s. Then $(3m - m)_2 = (2m)_2$ is the same as $(m)_2$, but shifted by one bit to the left. Hence in adding the two there is no carry if and only if there are no consecutive `1`s, which proves (a), by Lemma 2.1(a). If there are consecutive `1`s, then it is obvious that there are at least two carries, and this proves (b). □

As an aside, we obtain the following easy divisibility properties from Lemmas 4.1 and 4.2. Note that any positive integer of the form $4k+3$ has a binary representation ending in `11`.

Corollary 4.1. *For all integers* $k \geq 0$ *we have* $4 \mid u(4k+3)$*, and there are no integers* $n \geq 2$ *with* $u(n) \equiv 2 \pmod 4$.

Next we need a special case of a result in [12]. Let $0 \leq r \leq n$ be integers with binary representations

$$(n)_2 = a_l a_{l-1} \ldots a_1 a_0, \qquad (r)_2 = b_l b_{l-1} \ldots b_1 b_0,$$

and set

$$E_1 := \sum_{\substack{i=0 \\ a_{i+1}a_i = \texttt{11}}}^{l-1} (b_{i+1} + b_i), \qquad E_2 := \sum_{\substack{i=0 \\ a_{i+2}a_i = \texttt{11}}}^{l-2} (b_{i+2} + b_i).$$

Lemma 4.3 (Huard et al.)**.** *Let* $l \geq 2$*,* $a_1 a_0 \neq \texttt{11}$*, and suppose that* $\binom{n}{r}$ *is odd. Then*

$$\binom{n}{r} \equiv (-1)^{E_1} 5^{E_2} \pmod 8. \tag{4.6}$$

This result can be found in [12, p. 51]; the authors of that paper call (4.6) a "Davis-Webb congruence (mod 8)", after [5], where similar congruences modulo 4 were derived. We are now ready to prove the main result of this section.

Theorem 4.1. *For an integer* $m \geq 1$ *the congruence* (4.5) *holds if and only if the binary representation of* m *(padded right and left with* `0`*s) has no adjacent* `1`*s and has*

(a) *an odd number of strings* `00100` *or* `00101...0100`*, and*

(b) *an even number of strings* `010010`*.*

Proof. It is easy to see that the right-hand side of (4.6) is congruent to $-1 \pmod 8$ if and only if E_1 is odd and E_2 is even. We use Lemma 4.3 with $r = 2m$ and $n = 6m$. Then the condition $a_1 a_0 \neq \texttt{11}$ is clearly satisfied, and by hypothesis and Lemma 4.2(a) we know that $\binom{6m}{2m}$ is odd.

Let us first consider the sum E_1. For each 1 in $(2m)_2$ we have $b_i = 1, b_{i+1} = 0$, and $a_{i+1}a_i = 11$; hence the string 00100 is counted exactly once. If we have a string 00101...0100 in $(2m)_2$, then the corresponding string 011111...100 in $(6m)_2$ always has an even number of consecutive 1s. But this means that in E_1 an odd number of pairs $a_{i+1}a_i = 11$ sweeps over this string, and for each of these pairs we have exactly $b_{i+1} + b_i = 1$. Hence each string 00101...0100 gives an odd contribution to E_1, and this proves (a).

Next we consider the sum E_2. We can have $a_{i+2}a_i = 11$ in two different cases: (i) we have a string 00101...0100 in $(2m)_2$, with the corresponding string 011111...100 in $(6m)_2$. Then the terms $b_{i+2} + b_i$ are either 0 or 2, so the total contribution to E_2 of such a string is even and can thus be disregarded. (ii) we have a string 010010 in $(2m)_2$, with the corresponding string 110110 in $(6m)_2$. In this case the contribution to E_2 is odd, namely $b_{i+2} = 1, b_i = 0$. Thus the number of such string needs to be even, which proves (b). □

Examples: All the odd integers $m < 2^{11}$ that satisfy the conditions of Theorem 4.1, and thus the congruence (4.5), are listed in Table 2. Note that the primes in this list are exactly those (up to 2^{11}) that also appear in Table 1. We now consider two particular cases in detail:

(i) $m = p = 73$; $(73)_2 =$ 1001001. We have three "isolated" 1s, (i.e., at least two 0s between it and the next 1); hence E_1 is odd. We have two strings 1001, so E_2 is even.

(ii) $m = p = 1321$; $(1321)_2 =$ 10100101001. Here we have one isolated 1 and two strings 101, so E_1 is odd. Once again we see two strings 1001, so E_2 is even.

m	factored	m in binary	m	factored	m in binary
1	1	1	1041	$3 \cdot 347$	10000010001
5	5	101	1057	$7 \cdot 151$	10000100001
21	$3 \cdot 7$	10101	1089	$3^2 \cdot 11^2$	10001000001
73	73	1001001	1093	1093	10001000101
85	$5 \cdot 17$	1010101	1105	$5 \cdot 13 \cdot 17$	10001010001
273	$3 \cdot 7 \cdot 13$	100010001	1173	$3 \cdot 17 \cdot 23$	10010010101
293	293	100100101	1189	$29 \cdot 41$	10010100101
297	$3^3 \cdot 11$	100101001	1193	1193	10010101001
329	$7 \cdot 47$	101001001	1297	1297	10100010001
341	$11 \cdot 31$	101010101	1317	$3 \cdot 439$	10100100101
529	23^2	1000010001	1321	1321	10100101001
545	$5 \cdot 109$	1000100001	1353	$3 \cdot 11 \cdot 41$	10101001001
			1365	$3 \cdot 5 \cdot 7 \cdot 13$	10101010101

Table 2: Odd integers $m < 2^{11}$ satisfying (4.5)

The following corollary is now clear from Theorem 4.1 and the discussion at the beginning of this section.

Corollary 4.2. *The composite integer $n = 2p$, where p is an odd prime, is a solution of* (3.1) *if and only if p satisfies the conditions of Theorem 4.1.*

5. Growth and sign patterns of $u(n)$

In addition to the various divisibility and congruence properties studied above and in [4], the sequence $u(n)$ exhibits a sign pattern and a growth that are reminiscent of sequences generated by linear recurrence relations; see Table 3 for the first 30 values of $u(n)$. In this section we shall explain this behavior.

1. Computation. It is well known that the WZ algorithm (see, e.g., [22]) can be applied to many binomial sums to obtain closed formulas or recurrence relations. We have used the computer algebra system Maple 9.5 (the current version at the time of writing is Maple 11 [18]), which contains an implementation of the WZ algorithm, to obtain the recurrence relation

$$2(7n+4)(2n+3)(n+2)u(n+2)+(91n^3+325n^2+368n+128)u(n+1) \\ +16(7n+11)(2n+1)(n+1)u(n)=0. \tag{5.1}$$

This relation can be used to quickly compute the terms $u(n)$. However, the main limitation lies in the fact that even if only modular properties are investigated (such as (3.2) or (3.3)), the recurrence relation (5.1) does not reduce to a modular analogue. As we shall see below, the growth of the $u(n)$ is exponential, and above about $n = 4 \cdot 10^6$ the terms become prohibitively large, even though no more than three need to be stored at any given time. The computations were done with Maple 9.5. Up to our search limit of $n = 4 \cdot 10^6$ the only composite solutions to the congruence (3.1), 1145 in all, were of the form $2p$ or $5p$, where p is a prime. Contrary to the impression given by Table 1, solutions of the form $5p$ (646 in number) are more abundant than the 500 solutions of the form $2p$; the first composite solution, $n = 2 \cdot 5$, is counted in both categories.

n	$u(n)$	$s(n)$	n	$u(n)$	$s(n)$	n	$u(n)$	$s(n)$
0	1	+	10	-7001	-	20	159116983	+
1	-1	+	11	9316	-	21	-155628353	+
2	-1	-	12	22276	+	22	-720492928	-
3	8	-	13	-138412	+	23	3481793888	-
4	-17	-	14	268568	+	24	-5558713852	-
5	-1	+	15	189008	-	25	-9029921876	+
6	116	+	16	-2608913	-	26	71541001076	+
7	-344	+	17	6809417	-	27	-158672882224	+
8	239	+	18	-1814851	-	28	-45300345128	-
9	1709	-	19	-45852416	+	29	1370202238072	-

Table 3: The first 30 values of $u(n)$; $s(n) := \mathrm{sign}((-1)^n u(n))$

2. Growth and Asymptotics. If we divide both sides of (5.1) by $7n^3$, we see that the coefficients of the recurrence relation converge to 4, 13, and 32, respectively. The *characteristic equation* for (5.1) is therefore

$$4x^2+13x+32=0, \tag{5.2}$$

with roots

$$\alpha=\frac{-13+i7\sqrt{7}}{8}, \qquad \overline{\alpha}=\frac{-13-i7\sqrt{7}}{8}, \tag{5.3}$$

and obviously $|\alpha| = |\overline{\alpha}| = 2\sqrt{2}$. It is well known that the behavior of sequences of the type (5.1) can be determined by considering the roots of their characteristic

equations. Unfortunately, since (5.2) does not have a dominating root, the classical theorems of Poincaré and Perron (see, e.g., [13] or [14]) do not apply. Also, convergence of the coefficients of (5.1) (when divided by $7n^3$) to the coefficients of (5.2) is not fast enough to allow the use of some strong results, such as those in [14, Ch. 6]. However, we are able to apply Theorem 5 in [15] which gives the following result.

Corollary 5.1. *There exist two linearly independent solutions* $\{u_n^{(1)}\}, \{u_n^{(2)}\}$ *of the recurrence relation* (5.1) *such that*

$$\lim_{n\to\infty} \frac{u_{n+1}^{(1)}}{u_n^{(1)}} = \alpha, \qquad \lim_{n\to\infty} \frac{u_{n+1}^{(2)}}{u_n^{(2)}} = \overline{\alpha}.$$

A much stronger result was recently obtained by R. Noble [21] who used a generalized Riordan array related to the binomial sum $u(n)$ and applied methods of [23].

Theorem 5.1 (R. Noble)**.** *The sequence* $\{u(n)\}$ *satisfies the asymptotic expansion*

$$u(n) = \frac{d\alpha^n}{\sqrt{n}}\left(1 + \frac{c_1}{n} + \frac{c_2}{n^2} + \dots\right) + \frac{\overline{d}\overline{\alpha}^n}{\sqrt{n}}\left(1 + \frac{\overline{c_1}}{n} + \frac{\overline{c_2}}{n^2} + \dots\right), \tag{5.4}$$

with certain complex numbers $c_1, c_2, \dots$*, and*

$$d = \frac{1}{7^{1/4}\sqrt{\pi}} e^{i \arctan(8-3\sqrt{7})}. \tag{5.5}$$

It is easy to see from (5.3) that the argument of α is $\pi - \arctan(\frac{7\sqrt{7}}{13})$. If we set $d = |d|e^{i\delta}$ and $\alpha = 2\sqrt{2}e^{i(\pi-\theta)}$, where $\theta := \arctan(\frac{7\sqrt{7}}{13})$, then we have

$$d(-\alpha)^n + \overline{d}(-\overline{\alpha})^n = 2|d|2^{3n/2}\cos(\delta - n\theta),$$

and therefore, with (5.4) and (5.5),

$$(-1)^n u(n) = \frac{2}{7^{1/4}} \frac{2^{3n/2}}{\sqrt{\pi n}} \cos\big(n \arctan(\tfrac{7\sqrt{7}}{13}) - \arctan(8-3\sqrt{7})\big)\big(1 + O(\tfrac{1}{n})\big). \tag{5.6}$$

The identity (5.6) immediately gives an indication of the growth of the sequence $\{u(n)\}$. The period of the sign pattern of $(-1)^n u(n)$ is also easy to determine as $2\pi/\theta \simeq 6.55336$, which is consistent with Table 3.

6. Some open problems

1. Given that we were able to find a complete characterization of the primes p for which $2p$ is a solution of (3.1), it would be desirable to have a corresponding characterization of those p for which $5p$ solves (3.1). In Section 3 we saw that this is equivalent to p solving (3.3). The first sixteen such primes are 2, 5, 1549, 6701, 7699, 8527, 8929, 9043, 10243, 10459, 13963, 14249, 14369, 15349, 15877, and 19739. These are all such primes up to 20 000; there are a total of 646 up to $4 \cdot 10^6$.

It seems natural to consider the base-5 representation of these primes. However, there is no apparent pattern, and a reduction similar to the one that leads to (4.5) does not seem to be possible.

2. Are there infinitely many primes that satisfy conditions (a) and (b) in Theorem 4.1? This would imply that there are infinitely many composite solutions of (3.1). This problem appears to be of a similar level of difficulty as the question of the infinitude of Mersenne (`111...11` in binary) or Fermat primes (`100...01`).

3. Are there solutions of the form $n = qp$, with q a prime other than 2 or 5? Such solutions would be likely if there were a prime $q > 5$ with $u(q) = -1$; see Section 3. The question of *multiplicity* of a linear recurence sequence (with constant coefficients) is a difficult one, and there are numerous deep results, especially for the ternary case; see [8, Section 2.2] for results and references. Since by Corollary 5.1 the behavior of the sequence $u(n)$ is similar to that of the corresponding sequence with constant coefficients (namely the coefficients in (5.2)), with even greater similarity conjectured in (5.4), one would expect that there are at most finitely many q with $u(q) = -1$. It seems safe to conjecture that there will be no others beyond $q = 5$.

4. Are there solutions of (3.1) with three or more prime factors? Our calculations lead us to conjecture that there are none.

Acknowledgment

We would like to thank Rob Noble of Dalhousie University for allowing us to use his unpublished result, Theorem 5.1, which is part of his forthcoming doctoral thesis.

References

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

[2] H. Anton, *Die Elferprobe und die Proben für die Moduln 9, 13 und 101*, Archiv Math. Physik **49** (1869), 241–308.

[3] V. Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, and E. Jacobsthal, *On the divisibility of the difference between two binomial coefficients*. Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, pp. 42–54. Johan Grundt Tanums Forlag, Oslo, 1952.

[4] M. Chamberland and K. Dilcher, *Divisibility properties of a class of binomial Sums*, J. Number Theory **120** (2006), 349–371.

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

[6] K. S. Davis and W. A. Webb, *A binomial coefficient congruence modulo prime powers*, J. Number Theory **43** (1993), no. 1, 20–23.

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

[8] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, American Mathematical Society, Providence, Rhode Island, 2003.

[9] 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.

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

[11] C. Helou and G. Terjanian, *On Wolstenholme's theorem and its converse*. J. Number Theory **128** (2008), 475–499.

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

[13] W. G. Kelley and A. C. Peterson, *Difference Equations. An Introduction With Applications*. Second Edition. Academic Press, San Diego, 2001.

[14] R. J. Kooman, *Convergence Properties of Recurrence Sequences*, CWI Tract 83, Centrum voor Wiskunde en Informatica, Amsterdam, 1991.

[15] R. J. Kooman and R. Tijdeman, *Convergence properties of linear recurrence sequences*, Nieuw Arch. Wisk. (4) **8** (1990), 13–25.

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

[17] 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.

[18] Maple, `http://www.maplesoft.com/`.
[19] R. J. McIntosh, *A generalization of a congruential property of Lucas*, Amer. Math. Monthly **99** (1992), 231–238.
[20] R. J. McIntosh, *On the converse of Wolstenholme's theorem*, Acta Arith. **71** (1995), 381–389.
[21] R. Noble, *Personal communication*, 2009.
[22] M. Petkovšek, H. S. Wilf, and D. Zeilberger, $A=B$, AK Peters, Wellesley, MA, 1996.
[23] M. C. Wilson, *Asymptotics for generalized Riordan arrays*. 2005 International Conference on Analysis of Algorithms, 323–333 (electronic), Discrete Math. Theor. Comput. Sci. Proc., AD, Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2005.

Department of Mathematics and Statistics, 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`