A CONGRUENTIAL IDENTITY AND THE 2-ADIC ORDER OF LACUNARY SUMS OF BINOMIAL COEFFICIENTS

Gregory Tollisen
Department of Mathematics, Occidental College, 1600 Campus Road, Los Angeles, USA
tollisen@oxy.edu

Tamás Lengyel
Department of Mathematics, Occidental College, 1600 Campus Road, Los Angeles, USA
lengyel@oxy.edu

Received: 7/7/03, Revised: 3/26/04, Accepted: 4/1/04, Published: 4/2/04

Abstract

In this paper we obtain a universal lower bound on the 2-adic order of lacunary sums of binomial coefficients. By means of necessary and sufficient conditions, we determine the set of values for which the bound is achieved and show the periodicity of the set. We prove a congruential identity for the corresponding generating function. Our approach gives an alternative and transparent proof for some results derived recently by the second author and extends them. We also propose a conjecture that implies a recursion for calculating the 2-adic order of the lacunary sums for almost all values. A congruence in the style of Lucas is proved for the lacunary sums considered.

1. Introduction

We define the lacunary binomial sum

$$G_{n,l}(k) = \sum_{t=0}^{\lfloor k/n \rfloor} \binom{k}{l+nt}, \tag{1}$$

with $l : 0 \leq l \leq n-1$, and consider the situation where $n = p^m$, p prime, $m \geq 1$. Lacunary sums arise naturally in combinatorial contexts and have been studied in the past ([1], [2], [4], [5], [6], [8], [9], [10], and [11]). The p-adic order of $G_{p^m,l}(k)$ was explored in [6]. For $p > 2$, the exact p-adic order of $G_{p^m,l}(k)$ was obtained using a theorem of Stickelberger [4]. The 2-adic order of $G_{2^m,l}(k)$ was found on select regular sequences of values for k involving multiples of 2^{m-1} through use of the vertical generating function

$$g_{n,l}(x) = \sum_{k=0}^{\infty} G_{n,l}(k)x^k = \frac{x^l(1-x)^{n-l-1}}{(1-x)^n - x^n}$$

($n \geq 1$ and $l = 0, 1, \ldots, n-1$) in combination with multisection techniques to prove (among other results) that

$$\rho_2\left(G_{2^m,l}(k)\right) \geq \left\lfloor \frac{k}{2^{m-1}} \right\rfloor - 1 \tag{2}$$

for $l = 0$. Equality holds in (2) if $k = c2^m$ with $l = 0$ or 2^{m-1}, or if $k = c2^m + l$, $c2^{m-1} - 1$ with $l = 0, 1, \ldots, 2^m - 1$. That equality is not always attained is verified by the result (also proved in [6]) that $\rho_2\left(G_{2^m,0}(k)\right) = 2\left(\left\lfloor \frac{k}{2^{m-1}} \right\rfloor - 1\right)$ when $k = (2c-1)2^{m-1}$. In this paper, we prove that (2) is true for all k and l (cf. remarks in Section 3), and we characterize the necessary and sufficient conditions for equality (cf. corollary in Section 4).

Our primary focus is $(1+x)^k \bmod (x^{2^m} - 1)$ since the horizontal generating function $\sum_{l=0}^{2^m-1} G_{2^m,l}(k)x^l$ is obtained when $(1+x)^k$ is reduced mod $(x^{2^m} - 1)$ according to the congruence

$$\sum_{l=0}^{2^m-1} G_{2^m,l}(k)x^l \equiv (1+x)^k \bmod (x^{2^m} - 1).$$

Our main result is the theorem to be found in Section 3, wherein we identify the common power of 2 in the coefficients of $(1+x)^k \bmod (x^{2^m} - 1)$ for each value of k. After dividing out by the common power, we further reduce mod 2, to obtain a congruential factorization of the quotient into simple canonical factors based on the digits of the binary expansion of k. Our proof is by induction on m, and ultimately relies on repeated substitution of x^2 for x in congruences of the form $p(x) \equiv q(x) \bmod (x^{2^{m-1}} - 1)$ to yield $p(x^2) \equiv q(x^2) \bmod (x^{2^m} - 1)$ for polynomials $p(x)$ and $q(x)$.

Our approach is similar to some others used in analyzing congruential and divisibility properties, and p-adic orders of binomial coefficients [4]. In particular, a result by Lucas [7] states that

$$\binom{k}{l} \equiv \binom{\varepsilon_0}{\gamma_0}\binom{\varepsilon_1}{\gamma_1}\cdots\binom{\varepsilon_d}{\gamma_d} \bmod p,$$

where $k = \varepsilon_0 + \varepsilon_1 p + \ldots + \varepsilon_d p^d$ and $l = \gamma_0 + \gamma_1 p + \ldots + \gamma_d p^d$ in prime base p. To set a context for our result, in Section 2 we prove congruence (3) for $G_{p^m,l}(k)$, $p \geq 2$, à la Lucas [7], and explain why the congruence trivializes in the case of $G_{2^m,l}(k)$, thus leaving a gap that the corollary, in some sense, fills.

2. A congruence for $G_{p^m,l}(k)$, $p > 2$

Because we will be reducing polynomials mod p and mod $(x^{p^m} - 1)$, both for $p = 2$ and $p > 2$, followed by a further reduction mod $(p,\ x^{p^m} - 1)$, we begin by briefly explaining what we mean in each case. A polynomial $s(x) \in Z[x]$ is reduced to $r_1(x)$ mod p if $s(x) = pq_1(x) + r_1(x)$ where $q_1(x),\ r_1(x) \in Z[x]$ and the coefficients of $r_1(x)$ are

restricted to the values $0, 1, \ldots, p-1$. The polynomial $s(x)$ is reduced to $pq_2(x) + r_2(x)$ mod $(x^{p^m}-1)$ and to $r_2(x)$ mod $(p,\ x^{p^m}-1)$ if $s(x) = \left(x^{p^m}-1\right) q_3(x) + pq_2(x) + r_2(x)$ where $q_2(x),\ q_3(x),\ r_2(x) \in Z[x]$, $\deg(q_2(x)),\ \deg(r_2(x)) < p^m$, and the coefficients of $r_2(x)$ are restricted to the values $0, 1, \ldots, p-1$. Two polynomials are in the same congruence class if they reduce under the congruence modulus to the same polynomial. These define ring homomorphisms between $Z[x] \to Z_p[x] \to Z_p[x]/\left\langle x^{p^m}-1\right\rangle$ and between $Z[x] \to Z[x]/\left\langle x^{p^m}-1\right\rangle \to Z_p[x]/\left\langle x^{p^m}-1\right\rangle$ allowing us in each case to safely sequentially reduce.

We proceed by obtaining a Lucas-type result by a "Fine-styled" [3] argument. Let $k = \varepsilon_0 + \varepsilon_1 p + \ldots + \varepsilon_d p^d$ in base p. Kummer's carry counting shows that $p \left| \binom{p}{l} \right.$ if and only if $l \neq 0, p$, which immediately implies $(1+x)^p \equiv 1 + x^p \bmod p$, and after inducting on m, that $(1+x)^{p^m} \equiv 1 + x^{p^m} \bmod p$. Thus,

$$(1+x)^k \equiv (1+x)^{\varepsilon_0}(1+x^p)^{\varepsilon_1}(1+x^{p^2})^{\varepsilon_2}\ldots(1+x^{p^d})^{\varepsilon_d} \equiv \prod_{j=0}^{d}(1+x^{p^j})^{\varepsilon_j} \bmod p.$$

Now, by further reducing mod $(p,\ x^{p^m}-1)$, we use the fact that $1+x^{p^j} \equiv 2 \bmod (p,\ x^{p^m}-1)$ for $j \geq m$ to conclude that

$$\begin{aligned}
(1+x)^k &\equiv \left(\prod_{j=m}^{d}(1+x^{p^j})^{\varepsilon_j}\right)\left(\prod_{j=0}^{m-1}(1+x^{p^j})^{\varepsilon_j}\right) && \bmod p \\
&\equiv 2^{\varepsilon_m+\varepsilon_{m+1}+\ldots+\varepsilon_d}\prod_{j=0}^{m-1}\left(\sum_{\gamma_j=0}^{\varepsilon_j}\binom{\varepsilon_j}{\gamma_j}x^{\gamma_j p^j}\right) && \bmod (p,\ x^{p^m}-1) \\
&\equiv 2^{\varepsilon_m+\varepsilon_{m+1}+\ldots+\varepsilon_d}\sum_{l=0}^{p^m-1}\left(\prod_{j=0}^{d}\binom{\varepsilon_j}{\gamma_j}\right)x^l && \bmod (p,\ x^{p^m}-1)
\end{aligned}$$

where $l = \gamma_0 + \gamma_1 p + \ldots + \gamma_d p^d \leq p^m - 1$. After noting that $\sum_{l=0}^{p^m-1} G_{p^m,l}(k)x^l \equiv (1+x)^k \bmod (x^{p^m}-1)$ and using Fermat's little theorem, we immediately arrive at the

Lemma (à la Lucas). For $p > 2$ and prime, and for $k = \varepsilon_0 + \varepsilon_1 p + \ldots + \varepsilon_d p^d$ and $l = \gamma_0 + \gamma_1 p + \ldots + \gamma_{m-1}p^{m-1}$ in base p,

$$G_{p^m,l}(k) \equiv 2^{\varepsilon_m+\varepsilon_{m+1}+\ldots+\varepsilon_d}\binom{\varepsilon_0}{\gamma_0}\binom{\varepsilon_1}{\gamma_1}\cdots\binom{\varepsilon_{m-1}}{\gamma_{m-1}} \equiv 2^{\lfloor k/p^m \rfloor}\binom{k'}{l} \bmod p \tag{3}$$

where k' is the least nonnegative remainder of k when divided by p^m.

The lemma also can be proved by reducing all of the terms of (1) by applying Lucas' theorem and after factoring out $\binom{k'}{l}$, summing the quotients to get the other factor in (3). This idea was extended in the proof of Theorem 1 in [6].

We exclude $p = 2$, not because the lemma fails in this case, but because the power of 2 trivializes the identity to $G_{2^m,l}(k) \equiv 0 \bmod 2$ as soon as $k \geq 2^m$.

Note that [6, page 3] provides an alternative congruence mod p^{m+1} for $G_{p,l}(cp^m + i), 0 \leq i < l \leq p-1, m \geq 1$.

3. A congruential identity for $(1+x)^k$, $p=2$

Were we to devise a nontrivial result along the lines of Lucas for the case 2^m following an argument in the style of Fine, for each k we would first need to factor out the common power of 2 in $(1+x)^k \bmod (x^{2^m}-1)$, and then consider the remaining factor $\bmod(2,\ x^{2^m}-1)$ as we do in the following

Theorem. For $m \geq 1$ and $k \geq 2^{m-1}$, $2^{\lfloor k/2^{m-1} \rfloor -1} | (1+x)^k \bmod (x^{2^m}-1)$. Furthermore, for $m=1$ and $k \geq 1$: $(1+x)^k \equiv 2^{k-1}(1+x) \bmod (x^2-1)$. For $m \geq 2$ and $k \geq 1$, if $k = \varepsilon_0 + 2\varepsilon_1 + 4\varepsilon_2 + \ldots + 2^{m-1}\varepsilon_{m-1} + 2^m q$ with $0 \leq \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1} \leq 1$ then:

1. when $q=0$ (i.e., $1 \leq k < 2^m$):

$$(1+x)^k \equiv (1+\varepsilon_0 x)(1+\varepsilon_1 x^2)(1+\varepsilon_2 x^4)\ldots(1+\varepsilon_{m-2}x^{2^{m-2}})(1+\varepsilon_{m-1}x^{2^{m-1}}) \bmod 2,$$

2. when $q>0$ (i.e., $k \geq 2^m$):

$$\begin{aligned}(1+x)^k \equiv& \\ &\equiv 2^{\lfloor k/2^{m-1} \rfloor -1}(1+\varepsilon_0 x)(1+\varepsilon_1 x^2)(1+\varepsilon_2 x^4)\ldots \\ &\quad \ldots(1+\varepsilon_{m-2}x^{2^{m-2}})x^{2^{m-2}\varepsilon_{m-1}}(1+x^{2^{m-1}}) \qquad \bmod(2^{\lfloor k/2^{m-1} \rfloor}, x^{2^m}-1).\end{aligned} \tag{4}$$

Remarks. Before presenting the proof, we first note that the theorem instantly implies that $\rho_2\left(G_{2^m,l}(k)\right) \geq \left\lfloor \frac{k}{2^{m-1}} \right\rfloor - 1$. Second, we wish to draw the reader's attention to the last three factors in congruence (4) that, when combined, break the regular pattern followed by the preceding factors of lower degree, and thus, play a significant role in determining the conditions under which equality is reached, as will be explored in the corollary in the next section.

Proof. We cover the case $m=1$ with the preliminary

Claim 0. $(1+x)^k \equiv 2^{k-1}(1+x) \bmod (x^2-1)$, for $k \geq 1$.

Proof. Note that $(1+x)^2 \equiv 2(1+x) \bmod (x^2-1)$ and induct. □

The case when $q=0$ easily follows because in this case, if $k \geq 2^{m-1}$ then $2^{\lfloor k/2^{m-1} \rfloor -1} = 1$, and for $p \geq 0$, $(1+x)^{2^p} \equiv 1+x^{2^p} \bmod 2$. For the case when $q>0$, we proceed by induction on m.

BASE STEP: We begin by establishing the result for $m=2$ (i.e., $\bmod(x^4-1)$).

Claim 1. $2^{\lfloor k/2 \rfloor -1} | (1+x)^k \bmod (x^4-1)$, for $k \geq 4$.

Proof. Let $k = \varepsilon_0 + 2\varepsilon_1 + 4q$ and let $r = \left\lfloor \frac{k}{2} \right\rfloor = \varepsilon_1 + 2q$. Then

$$\begin{aligned}
(1+x)^{2r} &= \left[(1+x^2)+2x\right]^r = (2x)^r + \sum_{t=1}^{r} \binom{r}{t}(1+x^2)^t(2x)^{r-t} \\
&\equiv 2^r x^r + \sum_{t=1}^{r} \binom{r}{t} 2^{t-1}(1+x^2)2^{r-t}x^{r-t} && \bmod(x^4-1) \\
&\equiv 2^r x^r + 2^{r-1}(1+x^2)\left[\sum_{t=0}^{r}\binom{r}{t}x^{r-t} - x^r\right] && \bmod(x^4-1) \\
&\equiv 2^{r-1}\left[x^r(1-x^2) + (1+x^2)(1+x)^r\right] && \bmod(x^4-1)
\end{aligned}$$

where, in the first congruence of the sequence, Claim 0 was used with x^2 replacing x. Thus 2^{r-1} divides $(1+x)^k$ when reduced $\bmod(x^4-1)$. □

From now on, for notational convenience only, we move the power of 2 to the left.

Claim 2. $2^{-\lfloor k/2 \rfloor + 1}(1+x)^k \equiv (1+\varepsilon_0 x)x^{\varepsilon_1}(1+x^2) \bmod (2, x^4-1)$ for $k \geq 4$ (i.e., $q \geq 1$).

Proof. Continuing with the previous congruence,

$$\begin{aligned}
2^{-r+1}(1+x)^{2r} &\equiv x^r(1-x^2) + (1+x^2)(1+x)^r && \bmod(x^4-1) \\
&\equiv x^{\varepsilon_1+2q}(1-x^2) + (1+x^2)(1+x)^{\varepsilon_1+2q} && \bmod(x^4-1) \\
&\equiv x^{\varepsilon_1}\left[x^{2q}(1-x^2)\right] + (1+x)^{\varepsilon_1}\left[(1+x^2)\left((1+x)^2\right)^q\right] && \bmod(x^4-1) \\
&\equiv x^{\varepsilon_1}(x^{2q}+x^{2q+2}) + (1+x)^{\varepsilon_1}\left[(1+x^2)^2\left((1+x)^2\right)^{q-1}\right] && \bmod(2, x^4-1) \\
& && \text{(recall that } q \geq 1) \\
&\equiv x^{\varepsilon_1}(1+x^2) && \bmod(2, x^4-1)
\end{aligned}$$

Finish by multiplying both sides by $(1+x)^{\varepsilon_0} = 1 + \varepsilon_0 x$. □

INDUCTION STEP: We assume the theorem true for $m-1$ (i.e., $\bmod(x^{2^{m-1}}-1)$) and prove it true for m (i.e., $\bmod(x^{2^m}-1)$), $m \geq 3$.

Claim 3. Under the induction hypothesis, $2^{\left\lfloor k/2^{m-1} \right\rfloor - 1} | (1+x)^k \bmod (x^{2^m}-1)$, for $k \geq 2^m$ (i.e., $q \geq 1$).

Proof. Let $k = \varepsilon_0 + 2\varepsilon_1 + 4\varepsilon_2 + \ldots + 2^{m-1}\varepsilon_{m-1} + 2^m q$ and $r = \left\lfloor \frac{k}{2^{m-1}} \right\rfloor = \varepsilon_{m-1} + 2q$. Then,

$$(1+x)^{2^{m-1}r} = \left[(1+x^2)+2x\right]^{2^{m-2}r} = \sum_{t=0}^{2^{m-2}r} \binom{2^{m-2}r}{t}(1+x^2)^t(2x)^{2^{m-2}r-t}.$$

Now, from the induction hypothesis, $2^{\left\lfloor t/2^{m-2} \right\rfloor - 1} | (1+x^2)^t \bmod (x^{2^m}-1)$, by replacing x with x^2, so $2^{2^{m-2}r - t + \left\lfloor t/2^{m-2} \right\rfloor - 1}$ is a factor of the tth term of the sum, which takes on the minimum value of 2^{r-1} at $t = 2^{m-2}r$ and $t = 2^{m-2}r - 1$. Thus, $2^{r-1} | (1+x)^{2^{m-1}r} \bmod (x^{2^m}-1)$ and the claim follows. □

Claim 4. Under the induction hypothesis, $2^{-\lfloor k/2^{m-1}\rfloor+1}(1+x)^k \equiv (1+\varepsilon_0 x)(1+\varepsilon_1 x^2)(1+\varepsilon_2 x^4)\cdots(1+\varepsilon_{m-2}x^{2^{m-2}})x^{2^{m-2}\varepsilon_{m-1}}(1+x^{2^{m-1}}) \bmod (2, x^{2^m}-1)$, for $k \geq 2^m$ (i.e., $q \geq 1$).

Proof. Multiply both sides of the equation in Claim 3 by $2^{-r+1} = 2^{-\varepsilon_{m-1}-2q+1}$ and reduce $\bmod(x^{2^m}-1)$ to get

$$\begin{aligned}
2^{-r+1}(1+x)^{2^{m-1}r} &\equiv \sum_{t=0}^{2^{m-2}r-2} \tbinom{2^{m-2}r}{t} \left[2^{-r+1}(1+x^2)^t\right](2x)^{2^{m-2}r-t} + \\
&\quad + \tbinom{2^{m-2}r}{2^{m-2}r-1}\left[2^{-r+1}(1+x^2)^{2^{m-2}r-1}(2x)\right] + \tbinom{2^{m-2}r}{2^{m-2}r}\left[2^{-r+1}(1+x^2)^{2^{m-2}r}\right] \bmod (x^{2^m}-1) \\
&\equiv 2^{-r+1}(1+x^2)^{2^{m-2}r} && \bmod(2, x^{2^m}-1) \\
&&& \text{(all terms but the last are even)} \\
&\equiv 2^{-\varepsilon_{m-1}-2q+1}(1+x^2)^{2^{m-2}\varepsilon_{m-1}+2^{m-1}q} && \bmod(2, (x^2)^{2^{m-1}}-1) \\
&\equiv (x^2)^{2^{m-3}\varepsilon_{m-1}}(1+(x^2)^{2^{m-2}}) && \bmod(2, (x^2)^{2^{m-1}}-1) \\
&&& \text{(applying induction hyp. with } x^2 \text{ replacing } x) \\
&\equiv x^{2^{m-2}\varepsilon_{m-1}}(1+x^{2^{m-1}}) && \bmod(2, x^{2^m}-1)
\end{aligned}$$

Finish by multiplying both sides by $(1+x)^{\varepsilon_0+2\varepsilon_1+4\varepsilon_2+\ldots+2^{m-2}\varepsilon_{m-2}} \equiv (1+\varepsilon_0 x)(1+\varepsilon_1 x^2)(1+\varepsilon_2 x^4)\ldots(1+\varepsilon_{m-2}x^{2^{m-2}}) \bmod 2$. □

This truly concludes our proof of the theorem. □

4. A note, a corollary, and a conjecture

We conclude the paper with some comments, our primary application with consequences, and a conjecture.

Note. By replacing each instance of x with the $2^m \times 2^m$ forward shift permutation matrix

$$E = circ[0,1,0,\ldots,0] = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

and observing that $E^t \neq I$ for $t < 2^m$ while $E^{2^m} = I$, the theorem translates to modulo 2 congruential matrix identities for $(I+E)^k$ after removing the elementwise common power of 2 [11]. (In fact, if C is the ring of $2^m \times 2^m$ circulant matrices with integer coefficients, then $C \cong Z[x]/\langle x^{2^m}-1\rangle$, the isomorphism being $A \longmapsto p_A(x)$, where $p_A(x)$ is the auxiliary polynomial associated with the circulant matrix A.)

Corollary. For $m \geq 1,\ 0 \leq l < 2^m, k \geq 2^{m-1}$, we have $\rho_2(G_{2^m,\,l}(k)) \geq \left\lfloor \frac{k}{2^{m-1}} \right\rfloor - 1$, where $G_{n,l}(k)$ is as in (1). Furthermore, if

$$k = \varepsilon_0 + 2\varepsilon_1 + 4\varepsilon_2 + \ldots + 2^{m-1}\varepsilon_{m-1} + 2^m q$$

and

$$l = \gamma_0 + 2\gamma_1 + 4\gamma_2 + \ldots + 2^{m-1}\gamma_{m-1}$$

with $0 \le \varepsilon_i, \gamma_i \le 1$, then

1. when $q = 0$, equality holds if and only if $\varepsilon_i \ge \gamma_i$, $i = 0, 1, \ldots, m-1$, i.e., if and only if l, $k - l \ge 0$ have no carries when added.

2. when $q > 0$, equality holds if and only if $\varepsilon_i \ge \gamma_i$, $i = 0, 1, \ldots, m-3$, and $\gamma_{m-2} + \gamma_{m-1} \ge \varepsilon_{m-1}$ if $\varepsilon_{m-2} = 1$ or $\gamma_{m-2} = \varepsilon_{m-1}$ if $\varepsilon_{m-2} = 0$. (In fact, these two alternatives can be collapsed to $-\varepsilon_{m-2} \le \varepsilon_{m-1} - \gamma_{m-2} \le \varepsilon_{m-2}\gamma_{m-1}$.)

Case 1 can be written as

$$G_{2^m,l}(k) \equiv \binom{\varepsilon_0}{\gamma_0}\binom{\varepsilon_1}{\gamma_1}\cdots\binom{\varepsilon_{m-1}}{\gamma_{m-1}} \bmod 2,$$

while Case 2 can be partially represented by a similar form in line with congruence (4).

The proof of the corollary depends on using the theorem from Section 3 to determine the powers of $2^{-\lfloor k/2^{m-1} \rfloor + 1}(1+x)^k \bmod (2,\ x^{2^m} - 1)$ with nonzero coefficients. This is easily done, except perhaps when taking into account the last three factors in congruence (4). To handle these factors, one can simply but painstakingly check for all possible assignments of 0 and 1 to $\varepsilon_{m-2}, \varepsilon_{m-1}, \gamma_{m-2}$, and γ_{m-1}.

Note. The second case in the corollary with $l = 0, k \ge 2^m$, gives an instant proof of Conjecture 1 in [6]: the lower bound is achieved in (2) for 75% of the k values. Similarly, Conjectures 2 and 3 hold for the very same values.

Conjecture. The same process as above can be used to get a recursion for the lacunary binomial sums $G_{2^m,l}(k)$ themselves. We argue as follows:

$$(1+x)^{2q} = \left[2x + (1+x^2)\right]^q = \sum_{t=0}^{q} \binom{q}{t} (2x)^t (1+x^2)^{q-t}$$

Thus,

$$\begin{aligned}
\sum_{l=0}^{2^m-1} G_{2^m,l}(2q)x^l &\equiv \sum_{t=0}^{q} \tbinom{q}{t} 2^t x^t \left[\sum_{u=0}^{2^{m-1}-1} G_{2^{m-1},u}(q-t)(x^2)^u\right] \quad \bmod((x^2)^{2^{m-1}} - 1) \\
&\equiv \sum_{t=0}^{q} \sum_{u=0}^{2^{m-1}-1} \tbinom{q}{t} 2^t G_{2^{m-1},u}(q-t)x^{t+2u} \qquad \bmod(x^{2^m} - 1)
\end{aligned}$$

One then matches the powers of x. The result differs slightly depending on the parity of l. So, let $l = 2j + \varepsilon$ where ε is 0 or 1. Then, $G_{2^m,l}(2q) = \binom{q}{\varepsilon} 2^\varepsilon G_{2^{m-1},\,j}(q-\varepsilon) + \binom{q}{\varepsilon+2} 2^{\varepsilon+2} G_{2^{m-1},\,j-1}(q-\varepsilon-2) + \binom{q}{\varepsilon+4} 2^{\varepsilon+4} G_{2^{m-1},\,j-2}(q-\varepsilon-4) + \ldots$ where the second

subscript of G is taken $\bmod 2^{m-1}$. We conjecture, supported by numerical evidence, that for each m, $\rho_2(G_{2^m,l}(k))$ is equal to the diadic order of the leading term of the sum with a finite number of exceptions. Assuming the conjecture, we can find a simple recursion for the diadic order of the lacunary binomial sums. For $m > 2$,

$$\rho_2(G_{2^m,2j+\varepsilon}(2q)) = \begin{cases} \rho_2(G_{2^{m-1},\,j}(q)), & \text{if } \varepsilon = 0, \\ \rho_2(q) + 1 + \rho_2(G_{2^{m-1},\,j}(q-1)), & \text{if } \varepsilon = 1, \end{cases} \tag{5}$$

$$\rho_2(G_{2^m,l}(2q+1)) \begin{cases} = \min\left\{\rho_2(G_{2^m,\,l-1}(2q)), \rho_2(G_{2^m,\,l}(2q))\right\}, & \text{if the orders differ,} \\ \geq \rho_2(G_{2^m,\,l}(2q)) + 1, & \text{otherwise.} \end{cases}$$

The base of the recursion is the following

$$\rho_2(G_{4,l}(k)) = \begin{cases} 2\left(\left\lfloor \frac{k}{2} \right\rfloor - 1\right), & \text{if } k - 2l \equiv 2 \bmod 4, \\ \left\lfloor \frac{k}{2} \right\rfloor - 1, & \text{otherwise,} \end{cases}$$

valid for $k \geq \max\{2, l\}$, as can easily be proved. Again, numerical evidence suggests that for each $n = 2^m \geq 4$, the recursion (5) gives the exact diadic order of $G_{2^m,l}(k)$ except possibly for a finite number of small values for k where the recursion only gives a lower bound.

References

[1] D. S. Clark, On some abstract properties of binomial coefficients, *Amer. Math. Monthly* **89**(1982), 433–443.

[2] L. Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, 1974.

[3] N. J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54**(1947), 589–592.

[4] A. Granville, Binomial coefficients modulo prime powers, in preparation at `http://www.dms.umontreal.ca/~andrew` in `Binomial/index.html` or `Postscript/binomial.ps`, and `http://www.cecm.sfu.ca/organics/papers/granville/paper/binomial/html/binomial.html`

[5] F. T. Howard and R. Witt, Lacunary sums of binomial coefficients. *Applications of Fibonacci Numbers*, Vol 7: 185–195. Kluwer Academic Publishers, 1998.

[6] T. Lengyel, On the orders of lacunary binomial coefficient sums, *INTEGERS, Electronic Journal of Combinatorial Number Theory* **A3:3**(2003), 1–10.

[7] É. Lucas, Sur les congruences des nombres Euleriennes et des coefficients différentiels des functions trigonométrique, suivant un module premier, *Bull. Soc. Math. France* **6**(1878), 49–54.

[8] J. Riordan, *An Introduction to Combinatorial Analysis*, Wiley, New York, 1958.

[9] Z.-H. Sun and Z.-W. Sun, Fibonacci numbers and Fermat's last theorem, *Acta Arith.* **60**(1992), 371–388.

[10] Z.-W. Sun, On the sum $\sum_{k\equiv r \pmod m} \binom{n}{k}$ and related congruences, *Israel J. Math.* **128**(2002), 135–156.

[11] G. Tollisen and T. Lengyel, Averaging around the circle, manuscript, 2003.