Annales Mathematicae et Informaticae
41 (2013) pp. 121–136

Proceedings of the
15th International Conference on Fibonacci Numbers and Their Applications
Institute of Mathematics and Informatics, Eszterházy Károly College
Eger, Hungary, June 25–30, 2012

On divisibility properties of some differences of Motzkin numbers

Tamás Lengyel

Occidental College, Los Angeles, California, USA
lengyel@oxy.edu

Abstract

We discuss divisibility properties of some differences of Motzkin numbers M_n. The main tool is the application of various congruences of high prime power moduli for binomial coefficients and Catalan numbers combined with some recurrence relevant to these combinatorial quantities and the use of infinite disjoint covering systems.

We find proofs of the fact that, for different settings of a and b, more and more p-ary digits of $M_{ap^{n+1}+b}$ and M_{ap^n+b} agree as n grows.

Keywords: Catalan number, Motzkin number, harmonic number, divisibility

MSC: 11B83, 11B50, 11A07, 05A19

1. Introduction

The differences of certain combinatorial quantities, e.g., Motzkin numbers, exhibit interesting divisibility properties. Motzkin numbers are defined as the number of certain random walks or equivalently (cf. [2]) as

$$M_n = \sum_{k=0}^{n} \binom{n}{2k} C_k, n \geq 0, \tag{1.1}$$

where C_k is the kth Catalan number

$$C_k = \frac{1}{k+1}\binom{2k}{k}, k \geq 0.$$

We need some basic notation. Let n and k be positive integers, p be a prime, $d_p(k)$ and $\nu_p(k)$ denote the sum of digits in the base p representation of k and the highest power of p dividing k, respectively. The latter one is often referred to as the p-adic order of k. For the rational n/k we set $\nu_p(n/k) = \nu_p(n) - \nu_p(k)$.

We rely on the p-adic order of the differences of Catalan numbers $C_{ap^{n+1}+b} - C_{ap^n+b}$ (cf. Theorems 3.8 and 3.9) with a prime p, $(a,p) = 1$, and $n \geq n_0$ for some integer $n_0 \geq 0$.

As n grows, eventually more and more binary digits of M_{a2^n+b} and $M_{a2^{n+1}+b}$ agree, starting with the least significant bit, for every fixed $a \geq 1$ and $b \geq 0$, as stated by Theorem 2.3. We also determine lower bounds on the rate of growth in the number of matching digits in Corollary 2.4, Theorems 2.1 and 2.5. Conjecture 5.1 suggests finer details for $p = 2$. Conjectures 5.3 and 5.5 propose the exact value of $\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b})$ if $p = 2$, $a = 1$, and $b = 0, 1, 2$, as well as $\nu_p(M_{ap^{n+1}} - M_{ap^n})$ if $p = 3$ and $(a, 3) = 1$, or $p \geq 5$ prime and $a = 1$, in addition to half of the odd a values if $p = 2$ and n is odd. We present Conjectures 5.1-5.3 that concern upper and lower bounds on $\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b})$ and its exact value, respectively, with special interest in the cases with $a = 1$, $b = 0, 1, 2, 3$, and more generally, $b = 2^q - 1$, 2^q, and $2^q + 1, q \geq 1$. Further extensions and improvements are given in Theorems 5.6 and 5.7 (cf. [8]). All results involving the exact orders of differences or lower bounds on them can be easily rephrased in terms of super congruences for the underlying quantities.

Section 2 collects some of the main results (cf. Theorems 2.1 and 2.5) while Section 3 is devoted to known results and their direct consequences regarding congruential and p-adic properties of the binomial coefficients and Catalan numbers. We provide the proofs of Theorems 2.1 and 2.5 in Sections 4 and 5, respectively. We also prove Theorems 2.2-2.3 and state four conjectures (cf. Conjectures 5.1-5.3 and 5.5) related to Motzkin numbers in Section 5, including lower bounds on the order of differences for all primes.

2. Main results

In this section we list our main results regarding the differences of certain Motzkin numbers. Except for Theorem 2.3, they all determine lower bounds on the rate of growth in the number of matching p-ary digits in the differences.

Theorem 2.1. *For $p = 2$, $n \geq 2$, $a \geq 1$ odd, and $b = 0$ or 1, we have*

$$\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) = n - 1, \textit{if } n \textit{ is even}$$

and

$$\nu_2(M_{a2^{n+1}+b} - M_{a2^n} + b) \geq n, \textit{if } n \textit{ is odd.}$$

Theorem 2.2 provides us with a lower bound on $\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b})$ on a recursive fashion in b and potentially, it can give the exact order if $a = 1$.

Theorem 2.2. *For $a \geq 1$ odd and $n \geq n_0$ with some $n_0 = n_0(a, b) \geq 1$, we get that for $b \geq 2$ even*

$$\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) =$$

$$= \min\{\nu_2(M_{a2^{n+1}+b-1} - M_{a2^n+b-1}), \\ \nu_2(M_{a2^{n+1}+b-2} - M_{a2^n+b-2})\} - \nu_2(b+2)$$

if the two expressions under the minimum operation are not equal. However, it they are, then it is at least

$$\nu_2(M_{a2^{n+1}+b-1} - M_{a2^n+b-1}) + 1 - \nu_2(b+2).$$

On the other hand, if $b \geq 3$ is odd then we have

$$\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) = \nu_2(M_{a2^{n+1}+b-1} - M_{a2^n+b-1}) \tag{2.1}$$

if $\nu_2(M_{a2^{n+1}+b-2} - M_{a2^n+b-2}) + \nu_2(b-1) > \nu_2(M_{a2^{n+1}+b-1} - M_{a2^n+b-1})$, and

$$\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) = \nu_2(M_{a2^{n+1}+b-2} - M_{a2^n+b-2}) \\ + \nu_2(b-1)$$

if $\nu_2(M_{a2^{n+1}+b-2} - M_{a2^n+b-2}) + \nu_2(b-1) < \nu_2(M_{a2^{n+1}+b-1} - M_{a2^n+b-1})$, and otherwise, it is at least $\nu_2(M_{a2^{n+1}+b-1} - M_{a2^n+b-1})$. Note however the stipulation that in all equalities above, if the right hand side value is at least $n - 2\nu_2(b+2)$ then the equality turns into the inequality $\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) \geq n - 2\nu_2(b+2)$.

Theorem 2.2 guarantees that as n grows, eventually more and more binary digits of M_{a2^n+b} and $M_{a2^{n+1}+b}$ agree, starting with the least significant bit for every fixed $a \geq 1$ and $b \geq 0$.

Theorem 2.3. *For every $a \geq 1$, $b \geq 0$, and $K \geq 0$ integers, there exists an $n_0 = n_0(a, b, K)$ so that $\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) \geq K$ for all $n \geq n_0$.*

For the asymptotic growth of the Motzkin numbers we have $M_n \sim c3^n/n^{3/2}$ with some integer $c > 0$. Unfortunately, neither this fact nor Theorem 2.3 helps in assessing the rate of growth of matching digits, i.e., $\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b})$. However, Theorem 2.2 and $\sum'_{i \leq b+2} \nu_2(i) = \nu_2((b+2)!) = (b+2) - d_2(b+2)$, with the summation running through even values of i only, imply the following, although rather coarse, lower bound.

Corollary 2.4. *For $a \geq 1$ odd, $b \geq 0$, and $n \geq n_0$ with some $n_0 = n_0(a, b) \geq 1$, we have*

$$\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) \geq n - (b+2) + d_2(b+2).$$

Theorem 2.5 gives a lower bound on $\nu_3(M_{3^{n+1}+b} - M_{3^n+b})$ with $b = 0$ or 1, and $\nu_p(M_{p^{n+1}+b} - M_{p^n+b})$ for $p \geq 5$ and $0 \leq b \leq p-3$.

Theorem 2.5. *For $p \geq 3$ prime and $n \geq n_0$ with some integer $n_0 = n_0(p) \geq 0$, we have*

$$\nu_p(M_{p^{n+1}} - M_{p^n}) \geq n. \tag{2.2}$$

Assuming that $n \geq n_0$, for $p = 3$, we have

$$\nu_3(M_{3^{n+1}+1} - M_{3^n+1}) \geq n - 1,$$

and for $p \geq 5$, we have

$$\nu_p(M_{p^{n+1}+b} - M_{p^n+b}) \geq n$$

with $0 \leq b \leq p-3$.

3. Preparation

We note that there are many places in the literature where relevant divisibility and congruential properties of the binomial coefficients are discussed. Excellent surveys can be found in [5] and [11]. The following three theorems comprise the most basic facts regarding divisibility and congruence properties of the binomial coefficients. We assume that $0 \le k \le n$.

Theorem 3.1 (Kummer, 1852). *The power of a prime p that divides the binomial coefficient $\binom{n}{k}$ is given by the number of carries when we add k and $n-k$ in base p.*

Theorem 3.2 (Legendre, 1830). *We have*

$$\nu_p\big(\tbinom{n}{k}\big) = \tfrac{n-d_p(n)}{p-1} - \tfrac{k-d_p(k)}{p-1} - \tfrac{n-k-d_p(n-k)}{p-1} = \tfrac{d_p(k)+d_p(n-k)-d_p(n)}{p-1}.$$

In particular, $\nu_2(\binom{n}{k}) = d_2(k)+d_2(n-k)-d_2(n)$ represents the carry count in the addition of k and $n-k$ in base 2.

From now on M and N will denote integers such that $0 \le M \le N$.

Theorem 3.3 (Lucas, 1877). *Let $N = (n_d, \dots, n_1, n_0)_p = n_0 + n_1 p + \dots + n_d p^d$ and $M = m_0 + m_1 p + \dots + m_d p^d$ with $0 \le n_i, m_i \le p-1$ for each i, be the base p representations of N and M, respectively.*

$$\binom{N}{M} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\cdots\binom{n_d}{m_d} \bmod p.$$

Lucas' theorem has some remarkable extensions.

Theorem 3.4 (Anton, 1869, Stickelberger, 1890, Hensel, 1902). *Let $N = (n_d, \dots, n_1, n_0)_p = n_0 + n_1 p + \dots + n_d p^d, M = m_0 + m_1 p + \dots + m_d p^d$ and $R = N - M = r_0 + r_1 p + \dots + r_d p^d$ with $0 \le n_i, m_i, r_i \le p-1$ for each i, be the base p representations of $N, M,$ and $R = N-M$, respectively. Then with $q = \nu_p\big(\binom{N}{M}\big)$,*

$$(-1)^q \frac{1}{p^q}\binom{N}{M} \equiv \left(\frac{n_0!}{m_0! r_0!}\right)\left(\frac{n_1!}{m_1! r_1!}\right)\cdots\left(\frac{n_d!}{m_d! r_d!}\right) \bmod p.$$

Davis and Webb (1990) and Granville (1995) have independently generalized Lucas' theorem and its extension Theorem 3.4. For a given integer n and prime p, we define $(n!)_p = n!/(p^{\lfloor n/p \rfloor}\lfloor n/p \rfloor!)$ to be the product of positive integers not exceeding n and not divisible by p, and which is closely related to the p-adic Morita gamma function.

Theorem 3.5 (Granville, 1995 in [5]). *Let $N = (n_d, \dots, n_1, n_0)_p = n_0 + n_1 p + \dots + n_d p^d, M = m_0 + m_1 p + \dots + m_d p^d$ and $R = N - M = r_0 + r_1 p + \dots + r_d p^d$ with $0 \le n_i, m_i, r_i \le p-1$ for each i, be the base p representations of $N, M,$ and $R = N - M$, respectively. Let $N_j = n_j + n_{j+1} p + \dots + n_{j+k-1} p^{k-1}$ for each $j \ge 0$,* *i.e., the least positive residue of* $\lfloor N/p^j \rfloor \bmod p^k$ *with some integer* $k \geq 1$*; also make the corresponding definitions for* M_j *and* R_j*. Let* ϵ_j *be the number of carries when adding* M *and* R *on and beyond the* j*th digit. Then with* $q = \epsilon_0 = \nu_p\left(\binom{N}{M}\right)$*,*

$$\frac{1}{p^q}\binom{N}{M} \equiv (\pm 1)^{\epsilon_{k-1}} \left(\frac{(N_0!)_p}{(M_0!)_p (R_0!)_p}\right)\left(\frac{(N_1!)_p}{(M_1!)_p (R_1!)_p}\right)\cdots\left(\frac{(N_d!)_p}{(M_d!)_p (R_d!)_p}\right) \bmod p^k$$

where ± 1 *is* -1 *except if* $p = 2$ *and* $k \geq 3$*.*

We also use the following generalization of the Jacobstahl–Kazandzidis [1] congruences.

Theorem 3.6 (Corollary 11.6.22 [1])**.** *Let* M *and* N *such that* $0 \leq M \leq N$ *and* p *prime. We have*

$$\binom{pN}{pM} \equiv \begin{cases} \left(1 - \frac{B_{p-3}}{3} p^3 NM(N-M)\right)\binom{N}{M} & \bmod p^4 NM(N-M)\binom{N}{M}, \text{ if } p \geq 5, \\ (1 + 45NM(N-M))\binom{N}{M} & \bmod p^4 NM(N-M)\binom{N}{M}, \text{ if } p = 3, \\ (-1)^{M(N-M)} P(N,M)\binom{N}{M} & \bmod p^4 NM(N-M)\binom{N}{M}, \text{ if } p = 2, \end{cases}$$

where $P(N,M) = 1 + 6NM(N-M) - 4NM(N-M)(N^2 - NM + M^2) + 2(NM(N-M))^2$.

Remark 3.7. It is well known that $\nu_p(B_n) \geq -1$ by the von Staudt–Clausen theorem. If the prime p divides the numerator of B_{p-3}, i.e., $\nu_p(B_{p-3}) \geq 1$, or equivalently $\binom{2p}{p} \equiv 2 \bmod p^4$, then it is sometimes called a Wolstenholme prime [1]. The only known Wolstenholme primes up to 10^9 are $p = 16843$ and 2124679.

Based on the above theorems, we state some of the main tools regarding the differences of Catalan numbers (cf. [7] for details and proofs). For the p-adic orders we obtain the following theorem.

Theorem 3.8. *For any prime* $p \geq 2$ *and* $(a, p) = 1$*, we have*

$$\nu_p(C_{ap^{n+1}} - C_{ap^n}) = n + \nu_p\left(\binom{2a}{a}\right), \quad n \geq 1.$$

We can introduce an extra additive term $b \geq 1$ into Theorem 3.8.

Theorem 3.9. *For* $p = 2$*,* a *odd, and* $n \geq n_0 = 2$ *we have*

$$\nu_2(C_{a2^{n+1}+1} - C_{a2^n+1}) = n + \nu_2\left(\binom{2a}{a}\right) - 1,$$

and in general, for $b \geq 1$ *and* $n \geq n_0 = \lfloor \log_2 2b \rfloor + 1$

$$\nu_2(C_{a2^{n+1}+b} - C_{a2^n+b}) = n + \nu_2\left(\binom{2a}{a}\right) + \nu_2(g(b))$$

$$= n + d_2(a) + d_2(b) - \lceil \log_2(b+2) \rceil - \nu_2(b+1) + 1$$

where $g(b) = 2\binom{2b}{b}(b+1)^{-1}(H_{2b} - H_b - 1/(2(b+1))) = 2C_b(H_{2b} - H_b - 1/(2(b+1)))$ *with* $H_n = \sum_{j=1}^{n} 1/j$ *being the nth harmonic number.*

For any prime $p \geq 3$*,* $(a,p) = 1$*, and* $b \geq 1$ *we have that*

$$\nu_p(C_{ap^{n+1}+b} - C_{ap^n+b}) = n + \nu_p\left(\binom{2a}{a}\right) + \nu_p(g(b)),$$

with $n \geq n_0 = \max\{\nu_p(g(b)) + 2r - \nu_p(C_b) + 1, r+1\} = \max\{\nu_p(2(H_{2b} - H_b - 1/(2(b+1)))) + 2r + 1, r+1\}$ *and* $r = \lfloor \log_p 2b \rfloor$*.*

In general, for any prime $p \geq 2$*,* $(a,p) = 1, b \geq 1$*, and* $n > \lfloor \log_p 2b \rfloor$*, we have*

$$\nu_p(C_{ap^{n+1}+b} - C_{ap^n+b}) \geq n + \nu_p\left(\binom{2a}{a}\right) + \nu_p\left(\binom{2b}{b}\right) - \lfloor \log_p 2b \rfloor - \nu_p(b+1).$$

Note. Clearly, $\nu_p(g(b)) \geq 0$ for $1 \leq b \leq (p-1)/2$. We note that in general, for $b \geq 1$ we have $\nu_p(g(b)) \geq \nu_p(\binom{2b}{b}) - \lfloor \log_p 2b \rfloor - \nu_p(b+1)$ if $p \geq 2$ while $\nu_2(g(b)) = d_2(b) - \lceil \log_2(b+2) \rceil - \nu_2(b+1) + 1 = d_2(b+1) - \lceil \log_2(b+2) \rceil$ if $p = 2$.

We note that as a byproduct, we proved some generalization of the observation from [10] that for any $n \geq 2$ the remainders $C_{2^{n+m-1}-1} \bmod 2^n$ are equal for each $m \geq 0$ (see [9], [12], and [13],too) in [7]:

Theorem 3.10. *For any prime* $p \geq 2$*,* $(a,p) = 1, b \geq 0$*, we have that* $C_{ap^m+b} \bmod p^n$ *is constant for* $m \geq n + \nu_p(b+1) + \max\{0, \lfloor \log_p 2b \rfloor\}, n \geq 1$*.*

We also note that

$$\nu_2(C_k) = d_2(k) - \nu_2(k+1) = d_2(k+1) - 1 \tag{3.1}$$

holds, i.e., $\nu_2(C_{2^{n+1}}) = \nu_2(C_{2^n}) = 1$. It follows that C_k is odd if and only if $k = 2^q - 1$ for some integer $q \geq 0$.

4. The proof of Theorem 2.1

In this section we present

The proof of Theorem 2.1. We prove the case with $b = 0$ and then we note that the case with $b = 1$ is practically identical. Thus, we assume that $b = 0$.

First we deal with the case with $a = 1$. We use the identity (1.1)

$$M_{2^n} = \sum_{k=0}^{2^n} \binom{2^n}{2k} C_k,$$

rely on identity (3.1) and select an infinite incongruent disjoint covering system (IIDCS). The difference of the appropriate Motzkin numbers can be rewritten as

$$M_{2^{n+1}} - M_{2^n} = \sum_{k=1}^{2^{n-1}} \left(\binom{2^{n+1}}{2(2k)} C_{2k} - \binom{2^n}{2k} C_k \right) + \sum_{k \equiv 1 \bmod 2}^{2^n} \binom{2^{n+1}}{2k} C_k \tag{4.1}$$

after removing the superfluous term with $k = 0$ in the first sum. We break the first summation in (4.1) into parts according to the IIDCS $\{2^q \pmod{2^{q+1}}\}_{q \ge 0}$, which allows us to write every positive integer uniquely in the form of $2^q + 2^{q+1}K$ for some q and $K \ge 0$.

$$\begin{aligned}
&\sum_{k=1}^{2^{n-1}} \left(\binom{2^{n+1}}{2(2k)} C_{2k} - \binom{2^n}{2k} C_k \right) \\
&= \sum_{q=0}^{n-1} \sum_{\substack{k=2^q+2^{q+1}K \\ 0 \le K \le \frac{2^{n-q-1}-1}{2}}} \left(\binom{2^{n+1}}{2(2k)} C_{2k} - \binom{2^n}{2k} C_k \right) \\
&= \sum_{q=0}^{n-2} \sum_{\substack{k=2^q+2^{q+1}K \\ 0 \le K \le 2^{n-q-2}-1}} \left(\binom{2^{n+1}}{2(2k)} C_{2k} - \binom{2^n}{2k} C_k \right) \\
&+ (C_{2^n} - C_{2^{n-1}}).
\end{aligned} \tag{4.2}$$

We introduce the following quantities

$$M'_r(n, m) = \sum_{\substack{k \equiv r \bmod m \\ 1 \le k \le 2^n}} \binom{2^{n+1}}{2k} C_k$$

and focus on cases when m is a power of two.

The second summation in (4.1) is $M'_1(n, 2)$. Its 2-adic order is at least n according to

Theorem 4.1. *For integers $n \ge q \ge 1$, we have*

$$\nu_2(M'_{2^q}(n, 2^{q+1})) = n + 1 - q.$$

If $q = 0$ then $\nu_2(M'_1(n, 2)) = n$ if n is odd, otherwise the 2-adic order is at least $n + 1$.

We can gain more insight into the 2-adic structure of the terms of the sum (4.2) by checking how the 2-adic orders of the terms $\binom{2^n}{2k} C_k$ and $\binom{2^{n+1}}{2(2k)} C_{2k}$ with $k = 2^q + 2^{q+1}K$ behave in $M'_{2^q}(n-1, 2^{q+1})$ and $M'_{2^{q+1}}(n, 2^{q+2})$, respectively.

If $1 \le q \le n-1$ then both 2-adic orders are equal to $n - q + d_2(K)$. Indeed, the range for K is $0 \le K \le 2^{n-q-2} - 1$ if $q \le n-2$ and $K = 0$ if $q = n-1$ in both cases, and more importantly, the difference $A_{q,K} = \binom{2^{n+1}}{2(2k)} C_{2k} - \binom{2^n}{2k} C_k =$

$\binom{2^{n+1}}{2(2k)}(C_{2k}-C_k)+\left(\binom{2^{n+1}}{2(2k)}-\binom{2^n}{2k}\right)C_k$ has 2-adic order $n+d_2(K)$ by Theorems 3.1, 3.8, and 3.6. Note that $\nu_2(A_{q,K})$ is determined by the 2-adic order of the first term in the last sum, and it is given by combining $\nu_2\left(\binom{2^{n+1}}{2(2k)}\right)=n-1-q$ and $\nu_2(C_{2k}-C_k)=q+d_2(1+2K)=q+d_2(K)+1$. Therefore, $\nu_2(\sum_K A_{q,K})=n$ for each $q\geq 1$ and it is due to the term with $K=0$.

If $q=0$, i.e., $k=1+2K$, then $A_{0,K}=M_2'(n,4)-M_1'(n-1,2)$ and $\nu_2(A_{0,K})\geq n-1$ since $\nu_2\left(\binom{2^{n+1}}{4(1+2K)}C_{2+4K}\right)=n-1+d_2(3+4K)-1=n+d_2(K)$ and

$$\nu_2\left(\binom{2^n}{2(1+2K)}C_{1+2K}\right)=n-1+d_2(2+2K)-1=n-2+d_2(1+K)\geq n-1. \quad (4.3)$$

The latter minimum value is taken exactly for $n-1$ values of K since in the range $0\leq K\leq 2^{n-2}-1$ there are exactly $n-1$ terms with $K=2^r-1, r=0,1,\ldots,n-2$, leading to $d_2(K+1)=1$. Thus, the 2-adic order of the corresponding sum $\sum_K A_{0,K}$ is $n-1$ if n is even and at least n if n is odd.

The proof is now complete for the case $a=1$. The proof with an arbitrary $a\geq 1$ odd is very similar except it requires a more detailed analysis of the terms in (4.4) than we had in (4.1). In any case, the first term with $q=0$ in the right hand side of (4.2) and (4.5), i.e., $A_{0,K}=M_2'(n,4)-M_1'(n-1,2)$ and $A_{0,K,a}=M_{2,a}'(n,4)-M_{1,a}'(n-1,2)$ (cf. notation below), respectively, determines the 2-adic order.

We use the binary representation of $a=\sum_{i=0}^{\infty}a_i2^i=\sum_{i\in S}2^i$ with $0\in S=\{i|a_i=1\}$ since a is odd.

We rewrite the difference

$$M_{a2^{n+1}}-M_{a2^n}=\sum_{k=1}^{a2^{n-1}}\left(\binom{a2^{n+1}}{2(2k)}C_{2k}-\binom{a2^n}{2k}C_k\right)+\sum_{k\equiv 1 \bmod 2}^{a2^n}\binom{a2^{n+1}}{2k}C_k. \quad (4.4)$$

We break the first summation in (4.4) into parts according to the covering system used in (4.2)

$$\sum_{k=1}^{a2^{n-1}}\left(\binom{a2^{n+1}}{2(2k)}C_{2k}-\binom{a2^n}{2k}C_k\right)= \quad (4.5)$$
$$=\sum_{q=0}^{\lfloor\log_2 a2^{n-1}\rfloor}\sum_{\substack{k=2^q+2^{q+1}K\\ 0\leq K\leq\frac{a2^{n-q-1}-1}{2}}}\left(\binom{a2^{n+1}}{2(2k)}C_{2k}-\binom{a2^n}{2k}C_k\right).$$

Now we introduce

$$M_{r,a}'(n,m)=\sum_{\substack{k\equiv r \bmod m\\ 1\leq k\leq a2^n}}\binom{a2^{n+1}}{2k}C_k$$

and note that the second term in (4.4) is $M'_{1,a}(n,2)$. Its 2-adic order is at least n. In fact, for a general term in the sum $M'_{1,a}(n,2)$, we get that

$$\nu_2\left(\binom{a2^{n+1}}{2k}C_k\right) \geq (n+1-1)+(d_2(2+2K)-1) = n-1+d_2(1+K) \geq n \quad (4.6)$$

with $0 \leq k = 1+2K \leq a2^n$, i.e., $0 \leq K \leq a2^{n-1}-1$. We want equalities in (4.6) in order to determine $\nu_2(M'_{1,a}(n,2))$. While in the case of $a=1$ it trivially follows that $\nu_2(\binom{a2^{n+1}}{2k}) = n$, now we have to deal with the possibility that $2k > 2^{n+1}$. By Theorem 3.1, the first inequality turns into equality exactly if

$$K = j + \sum_{i\in S'\subseteq S\setminus\{0\}} 2^{i+n-1}$$

with $0 \leq j \leq 2^{n-1}-1$, while the second one becomes an equality when $d_2(K+1) = |S'| + d_2(j+1) = 1$, i.e., $S' = \emptyset$ and $j = 2^r - 1$ and thus, $K = 2^r - 1$ with $r = 0, 1, \ldots, n-1$. Therefore, this case turns out to be identical to that of $a = 1$ and hence, $\nu_2(M'_{1,a}(n,2)) \geq n$ with equality if and only if n is odd. (By the way, this argument is also used at the end of the proof of Theorem 4.1 below. Note that Theorem 4.1 remains valid even after introducing the parameter a, i.e., if we replace $M'_{2^q}(n,2^{q+1})$ with $M'_{2^q,a}(n,2^{q+1})$, cf. Theorem 4.2.)

Now we turn to the analysis of (4.5). We have three cases: either $1 \leq q \leq n-1$, or $q \geq n$, or $q = 0$. We consider the difference with $k = 2^q + 2^{q+1}K$

$$\begin{aligned} A_{q,K,a} &= \binom{a2^{n+1}}{2(2k)}C_{2k} - \binom{a2^n}{2k}C_k \\ &= \binom{a2^{n+1}}{2(2k)}(C_{2k}-C_k) + \left(\binom{a2^{n+1}}{2(2k)} - \binom{a2^n}{2k}\right)C_k. \end{aligned} \quad (4.7)$$

If $1 \leq q \leq n-1$ then it has 2-adic order $n + d_2(K)$ by Theorems 3.1, 3.8, and 3.6. Note that $\nu_2(A_{q,K,a})$ is determined by the 2-adic order of the first term in the last sum and it is given by combining $\nu_2(\binom{a2^{n+1}}{2(2k)}) = n-1-q$ and $\nu_2(C_{2k}-C_k) = q + d_2(1+2K) = q + d_2(K) + 1$. Therefore, $\nu_2(\sum_K A_{q,K,a}) = n$ for each $q \geq 1$ and it is due to the term with $K = 0$.

If $q \geq n$ then both terms of the last sum in (4.7) have a 2-adic order of at least $n+1$ by Theorems 3.1, 3.8, and 3.6. For example, for the first term we see that $\nu_2(C_{2k}-C_k) = q + d_2(1+2K) \geq n+1+d_2(K) \geq n+1$.

If $q = 0$, i.e., $k = 1+2K$, then $\nu_2(A_{0,K,a}) = n-1$ since $\nu_2(\binom{a2^{n+1}}{4(1+2K)}C_{2+4K}) = n-1+d_2(3+4K)-1 = n+d_2(K)$ and

$$\nu_2\left(\binom{a2^n}{2(1+2K)}C_{1+2K}\right) \geq n-1+d_2(2+2K)-1 = n-2+d_2(1+K) \geq n-1. \quad (4.8)$$

In a similar fashion to (4.6), the latter minimum value is taken exactly for $n-1$ values of K since in the range $0 \le K \le a2^{n-2}-1$ there are exactly $n-1$ terms with $K=2^r-1, r=0,1,\dots,n-2$, leading to $d_2(K+1)=1$ so that $\nu_2\big(\binom{a2^n}{2(1+2K)}\big)=n-1$. Thus, the 2-adic order of the corresponding sum $\sum_K A_{0,K,a}$ is $n-1$ if n is even and at least n if n is odd.

If $b=1$ then we observe that the 2-adic orders of $\binom{a2^n+1}{2k}$ and $\binom{a2^n}{2k}$ are equal. By switching from $a2^n$ and $a2^{n+1}$ to $a2^n+1$ and $a2^{n+1}+1$, respectively, the proof is almost identical to that of the case with $b=0$. Note that the only term that requires some extra work is the second term $\big(\binom{a2^{n+1}+1}{2(2k)}-\binom{a2^n+1}{2k}\big)C_k$ in the revised version of (4.7). In fact, its 2-adic order is at least n (more precisely, after making b_1 more specific below, it is $\nu_2\big(2k\binom{a2^n}{2k}\big)$), as it follows by Theorem 3.6:

$$\begin{aligned}\binom{a2^{n+1}+1}{4k}-\binom{a2^n+1}{2k}&=\\ &=\frac{a2^{n+1}+1}{a2^{n+1}+1-4k}\binom{a2^{n+1}}{4k}-\frac{a2^n+1}{a2^n+1-2k}\binom{a2^n}{2k}\\ &=\frac{a2^{n+1}+1}{a2^{n+1}+1-4k}\binom{a2^n}{2k}(1+b_12^{n+1})-\frac{a2^n+1}{a2^n+1-2k}\binom{a2^n}{2k}\\ &=\left(\frac{a2^{n+1}+1}{a2^{n+1}+1-4k}-\frac{a2^n+1}{a2^n+1-2k}+b_22^{n+1}\right)\binom{a2^n}{2k}\\ &\equiv\frac{2k}{(a2^{n+1}+1-4k)(a2^n+1-2k)}\binom{a2^n}{2k}\equiv a2^n\binom{a2^n-1}{2k-1}\\ &\equiv 0 \pmod{2^n}\end{aligned}$$

where $b_i, i=1$ and 2 are some numbers with $\nu_2(b_i)\ge 0$. □

Apparently, cases with $b\ge 2$ call for more refined methods. It also appears that proving Conjecture 5.5 for $p=2$ might require congruences modulo 2^{n+1} for both $\binom{a2^{n+1}}{2(2k)}(C_{2k}-C_k)$ in (4.7) and $\binom{a2^n}{2(1+2K)}C_{1+2K}$ in (4.8). In fact, it helped proving Theorem 5.6 (cf. Section 5 below).

Now we prove Theorem 4.1.

The proof of Theorem 4.1. For the 2-adic orders of the terms of $M'_{2^q}(n,2^{q+1})$ with $1\le q\le n$, we get that

$$\begin{aligned}\nu_2\left(\binom{2^{n+1}}{2k}C_k\right)=n-\nu_2(k)+\nu_2(C_k)&=n-q+d_2(1+2^q+2^{q+1}K)-1\\ &=n-q+1+d_2(K)\ge n-q+1,\end{aligned}$$

and the lower bound is met exactly if $K=0$.

If $q=0$ then we have $\nu_2(M'_1(n,2))\ge n$ by (4.3). In fact, as it was explained above in the proof of Theorem 2.1 but now using $n+1$ rather than n and $0\le k=$

$1 + 2K \le 2^n$, i.e., $0 \le K \le 2^{n-1} - 1$ in the summation resulting in $M_1'(n, 2)$, the minimum 2-adic value n is taken by n terms with $K = 2^r - 1, r = 0, 1, \ldots, n-1$. Therefore, for the 2-adic order of the sum, we get n exactly if n is odd. □

We also have the following

Theorem 4.2. *For integers $n \ge q \ge 1$, we have*

$$\nu_2(M'_{2^q,a}(n, 2^{q+1})) = n + 1 - q.$$

If $q = 0$ then $\nu_2(M'_{1,a}(n, 2)) = n$ if n is odd, otherwise the 2-adic order is at least $n + 1$.

We omit the proof but mention that the case with $q = 0$ has already been proven in the proof of Theorem 2.1 by using (4.6) while the case with $1 \le q \le n$ can be taken care of similarly to the proof of Theorem 4.1.

5. More proofs, facts, and conjectures for Motzkin numbers

Here we present the proofs of Theorems 2.2, 2.3, and 2.5, and four conjectures on the order of the difference of certain Motzkin numbers including cases with any prime $p \ge 3$.

Proof of Theorem 2.2. We use a recurrence for the Motzkin numbers:

$$M_m = \frac{3(m-1)M_{m-2} + (2m+1)M_{m-1}}{m+2}, m \ge 0, \tag{5.1}$$

with $m = a2^{n+1} + b$ and $a2^n + b$. We take the difference and simplify it. It turns out that the common denominator on the right hand side is odd when b is odd and has 2-adic order $2\nu_2(b + 2)$ when b is even. In the numerator only the two terms $3(b-1)(b+2)\big(M_{a2^{n+1}+b-2} - M_{a2^n+b-2}\big)$ and $(2b+1)(b+2)\big(M_{a2^{n+1}+b-1} - M_{a2^n+b-1}\big)$, and possibly two additive terms with 2-adic order at least n matter (due to the possibility that either $\nu_2(2^n 3M_{a2^{n+1}+b-1}) = n$ or $\nu_2(2^n 9M_{a2^{n+1}+b-2}) = n$ or both). The details are straightforward. □

Proof of Theorem 2.3. We prove by induction on b for any fixed $a \ge 1$ odd since it suffices to consider only such values of a. The cases with $b = 0$ and 1 are covered by Theorem 2.1. Assume that the statement is true for all values $0, 1, \ldots, b-2, b-1$. We set $K' = K + 2\nu_2(b + 2)$ and $n_0 = n_0(a, b, K) = \max\{n_0(a, b-2, K'), n_0(a, b-1, K')\}$ and apply Theorem 2.2 which yields that $\nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) \ge K' - 2\nu_2(b + 2) = K$ for $n \ge n_0(a, b, K)$. □

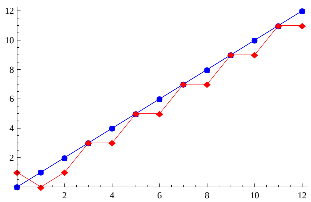
Further numerical evidence suggests a refinement of Corollary 2.4 on the rate of growth (cf. Figure 1 for illustration).

Conjecture 5.1. *For all integers $a \geq 1$ odd, $b \geq 0$ and n sufficiently large, there exist two constants $c_1(a,b)$ and $c_2(a,b)$ so that $n - c_1(a,b) \leq \nu_2(M_{a2^{n+1}+b} - M_{a2^n+b}) \leq n + c_2(a,b)$. In particular, we have $c_1(1,b) \leq c \log_2 b$ with some constant $c > 0$, $c_2(1,b) \leq 1$, and $c_1(1, 2^q - 1) \leq q$ and $c_2(1, 2^q) \leq -1$ for $q \geq 2$.*

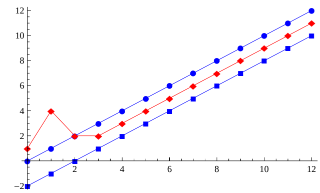
We also believe that following conjecture is true.

Conjecture 5.2. *The sequences $\{\nu_2(M_{2^{n+1}+b} - M_{2^n+b})\}_{n \geq n_0}$ with $b = 2^q$ and $b = 2^q + 1, q \geq 1$, become identical for some sufficiently large $n_0 = n_0(q)$.*

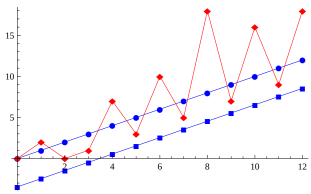
This means that, in this special case, equality (2.1) holds with a value which is less than n in Theorem 2.2. By the way, this seems to happen in many cases when we compare $M_{2^{n+1}+b} - M_{2^n+b}$ with $M_{2^{n+1}+b+1} - M_{2^n+b+1}$ with b even.



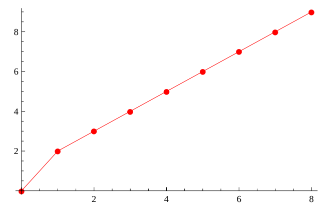
(a) $p = 2, a = 1, b = 1$ (which agrees with $a = 1, 5, 9$, or 13, and $b = 0$ for $n \geq 1$, cf. Theorem 2.1, Conjectures 5.3 and 5.5)



(b) $p = 2, a = 1, b = 4$ (which agrees with $a = 1, b = 5$ for $n \geq 3$, cf. Conjecture 5.2)



(c) $p = 2, a = 3, b = 11$, cf. Conjecture 5.1



(d) $p = 3, a = 2, b = 0$, cf. Conjecture 5.5

Figure 1: The function $\nu_p(M_{ap^{n+1}+b} - M_{ap^n+b}), 0 \leq n \leq 12$ (with $y = n$ and $n - \log_2 b$ included for $p = 2$)

We have a "conditional proof" of Conjecture 5.2 under assumptions on $c_1(1, 2^q - 1)$ and $c_2(1, 2^q)$. The inequalities of Conjecture 5.1 combined with equality (2.1) would already prove Conjecture 5.2 for $q \geq 2$. Indeed, in this case we have $\nu_2(M_{2^{n+1}+2^q+1} - M_{2^n+2^q+1}) = \nu_2(M_{2^{n+1}+2^q} - M_{2^n+2^q})$ since $\nu_2(M_{2^{n+1}+2^q-1} - M_{2^n+2^q-1}) + \nu_2(2^q + 1 - 1) \geq n - c_1(1, 2^q - 1) + q \geq n > n - 1 \geq n + c_2(1, 2^q) \geq \nu_2(M_{2^{n+1}+2^q} - M_{2^n+2^q})$.

This argument would not work for $q = 1$, i.e., for $b = 2$ and 3. However, by assuming the "right" patterns for $b = 1$ and 2, we can prove the case with $b = 3$.

Indeed, Conjecture 5.3 and equality (2.1) immediately imply the statement of Conjecture 5.2 for n odd and $b = 3$. If n is even and $b = 3$ then a slight fine tuning in the proof of Theorem 2.2 will suffice since $\nu_2(M_{2^{n+1}+2}) = 1$ for $n \geq 3$ and $\nu_2(M_{2^{n+1}+1}) = 0$ for $n \geq 1$ (by Conjecture 5.3 and the facts that $\nu_2(M_{18}) = 1$ and $\nu_2(M_5) = 0$).

We add that Theorem 2.1 states a similar fact about identical sequences with $b = 0$ and 1 for a odd and n even.

Conjecture 5.3. *If $n \geq 2$, and $b = 0$ or 1 then*

$$\nu_2(M_{2^{n+1}+b} - M_{2^n+b}) = \begin{cases} n-1, & \text{if } n \text{ is even,} \\ n, & \text{if } n \text{ is odd.} \end{cases}$$

If $n \geq 3$, and $b = 2$ then

$$\nu_2(M_{2^{n+1}+b} - M_{2^n+b}) = \begin{cases} n, & \text{if } n \text{ is even,} \\ n-2, & \text{if } n \text{ is odd.} \end{cases}$$

Remark 5.4. The case with $b = 0$ or 1, and $n \geq 2$ even has already been proven as part of Theorem 2.1 (with $a = 1$). On the other hand, we obtained only a lower bound if n is odd and otherwise, this case remains open. Therefore, the former case can be left out from the conjecture and was included only for the sake of uniformity.

The case with $a = 1$ and $b = 0$ is further extended in

Conjecture 5.5. *For $p = 2$, $a \equiv 1 \pmod 4$, and $n \geq 2$, we have*

$$\nu_2(M_{a2^{n+1}} - M_{a2^n}) = n, \text{ if } n \text{ is odd.}$$

For $p = 3$, $(a, 3) = 1$, and $n \geq n_0 = n_0(a)$ with some integer $n_0(a) \geq 0$, we have

$$\nu_3(M_{a3^{n+1}} - M_{a3^n}) = n + \nu_3\left(\binom{2a}{a}\right).$$

For $p \geq 5$ prime and $n \geq n_0 = n_0(p)$ with some integer $n_0(p) \geq 0$, we have

$$\nu_p(M_{p^{n+1}} - M_{p^n}) = n.$$

The panels (a) and (d) of Figure 1 demonstrate this conjecture in some cases with $0 \leq n \leq 12$. If $p = 2$, $a \geq 1$ any odd, and $n \geq 2$ even then the 2-adic order is $n - 1$ as it has already been proven in Theorem 2.1.

The proof of Theorem 2.5. We give only a sketch of the proof.

We prove the case with $b = 0$ first and use the IIDCS

$$\{ip^q \pmod{p^{q+1}}\}_{i=1,2,\dots,p-1;q\geq 0}$$

which allows us to write every positive integer uniquely in the form of $ip^q + Kp^{q+1}$ with some integers $K \geq 0$, i, and q. In a similar fashion to the proof of Theorem 2.1, the difference of the appropriate Motzkin numbers can be rewritten as

$$
\begin{aligned}
M_{p^{n+1}} - M_{p^n} &= \sum_{k=1}^{p^n/2} \left(\binom{p^{n+1}}{p(2k)} C_{pk} - \binom{p^n}{2k} C_k \right) + \sum_{i=1}^{p-1} \left(\sum_{k \equiv i \bmod p}^{p^{n+1}/2} \binom{p^{n+1}}{2k} C_k \right) \\
&= \sum_{q=0}^{n-1} \sum_{i=1}^{p-1} \left(\sum_{\substack{k=ip^q+Kp^{q+1} \\ 0 \leq K \leq \frac{p^{n-q}-2i}{2p}}} \left(\binom{p^{n+1}}{p(2k)} C_{pk} - \binom{p^n}{2k} C_k \right) \right) \qquad (5.2) \\
&+ \sum_{i=1}^{p-1} \left(\sum_{k \equiv i \bmod p}^{p^{n+1}/2} \binom{p^{n+1}}{2k} C_k \right) \qquad (5.3)
\end{aligned}
$$

after removing the superfluous term with $k = 0$ in the first sum. The first term (5.2) can be rewritten as

$$
\begin{aligned}
&\sum_{q=0}^{n-1} \sum_{i=1}^{p-1} \sum_{\substack{k=ip^q+Kp^{q+1} \\ 0 \leq K \leq \frac{p^{n-q}-2i}{2p}}} \left(\binom{p^{n+1}}{p(2k)} C_{pk} - \binom{p^n}{2k} C_k \right) \\
&= \sum_{q=0}^{n-1} \sum_{i=1}^{p-1} \sum_{\substack{k=ip^q+Kp^{q+1} \\ 0 \leq K \leq \frac{p^{n-q}-2i}{2p}}} \left(\binom{p^{n+1}}{p(2k)} (C_{pk} - C_k) + \left(\binom{p^{n+1}}{p(2k)} - \binom{p^n}{2k} \right) C_k \right).
\end{aligned}
$$

For the p-adic order of every term in the summation, we obtain that $\nu_p(\binom{p^{n+1}}{p(2k)}(C_{pk} - C_k)) \geq n - q + q = n$ by Theorem 3.8, and $\nu_p((\binom{p^{n+1}}{p(2k)} - \binom{p^n}{2k})C_k) \geq n + 2$ by Theorem 3.6 and Remark 3.7.

Clearly, the p-adic order of every term in (5.3) is at least $n + 1$.

Unfortunately, the above treatment cannot be easily extended to higher values of b, however, recurrence (5.1) comes to the rescue. Indeed, if $p = 3$ and $b = 1$, or $p \geq 5$ and $1 \leq b \leq p - 3$ then we use (5.1) with $m = p^{n+1} + b$ and $p^n + b$, and by easily adapting the proof of Theorem 2.2, we prove the statement step by step for $b = 1$, then for $b = 2$, ..., and finally for $b = p - 3$. In the initial case of $b = 1$, the multiplying factor $m - 1$ of M_{m-2} in (5.1) is divisible by p^n in both settings of m while the terms with M_{m-1} are covered by the case of $b = 0$. Starting with $b = 2$, we can use the already proven statement with $b - 1$ and $b - 2$. This proof cannot be directly extended beyond $b = p - 3$ since the common denominator in the recurrence has p-adic order $2\nu_p(b + 2)$, and this is the reason for the potential drop in the 3-adic order when $b = 1$. □

Note that we have recently succeeded in proving the following extensions and improvements to Conjecture 5.5 and Theorem 2.5 in [8], by applying congruential recurrences and refining the techniques used in this paper. The last part of the first theorem confirms Conjecture 5.5 for $p = 2$ and $a = 1$ given that n is odd. The case with n even has been settled by Theorem 2.1.

Theorem 5.6. *For $p = 2$, we have that*

$$M(2^{n+1}) - M(2^n) = \begin{cases} 3 \cdot 2^{n-1} \bmod 2^{n+1}, & \text{if } n \geq 4 \text{ and even,} \\ 2^n \bmod 2^{n+1}, & \text{if } n \geq 3 \text{ and odd.} \end{cases}$$

For $n \geq 2$, we have

$$\nu_2(M(2^{n+1}) - M(2^n)) = \begin{cases} n-1, & \text{if } n \text{ is even,} \\ n, & \text{if } n \text{ is odd.} \end{cases}$$

Theorem 5.7. *For any prime $p \geq 3$ and integer $n \geq 2$, we have that $\nu_p(M(p^{n+1}) - M(p^n)) = n$. In particular, with the Legendre symbol $(\frac{p}{3})$, we have*

$$M(p^{n+1}) - M(p^n) \equiv \begin{cases} \frac{p-1}{2} p^n \bmod p^{n+1}, & \text{if } (\frac{p}{3}) \equiv 0 \text{ or } 1 \bmod p, \\ (\frac{p+1}{4} + (-1)^n \frac{p-3}{4}) p^n \bmod p^{n+1}, & \text{if } (\frac{p}{3}) \equiv -1 \bmod p. \end{cases}$$

Acknowledgements. The author wishes to thank Gregory P. Tollisen for his helpful comments.

References

[1] H. Cohen, *Number Theory, vol 2: Analytic and Modern Tools*, Graduate Texts in Mathematics, Springer, 2007

[2] Emeric Deutsch and Bruce E. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, *Journal of Number Theory* Vol. 117 (2006), 191–215.

[3] A. Eswarathasan and E. Levine, p-integral harmonic sums, *Discrete Math.* Vol. 91(1991), 249–257.

[4] S.-P. Eu, S.-C. Liu, and Y.-N. Yeh, Catalan and Motzkin numbers modulo 4 and 8, *European J. Combin.* Vol. 29(2008), 1449–1466.

[5] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic mathematics* (Burnaby, BC, 1995), volume 20 of CMS Conf. Proc., 253–276, Amer. Math. Soc., Providence, RI, 1997. Electronic version (a dynamic survey): `http://www.dms.umontreal.ca/~andrew/Binomial/`

[6] K. S. Kedlaya, B. Poonen, and R. Vakil, *The William Lowell Putnam Mathematical Competition*, 1985–2000, Mathematical Association of America, Washington, DC, 2002

[7] T. Lengyel, On divisibility properties of some differences of the central binomial coefficients and Catalan numbers, *INTEGERS, Electronic Journal of Combinatorial Number Theory* Vol. 13 (2013), #A10, 1–20.

[8] T. Lengyel, Exact p-adic orders for differences of Motzkin numbers, manuscript, 2012

[9] H.-Y. Lin, Odd Catalan numbers modulo 2^k, *INTEGERS, Electronic Journal of Combinatorial Number Theory* Vol. 11 (2011), #A55, 1–5.

[10] Shu-Chung Liu and Jean C.-C. Yeh, Catalan Numbers Modulo 2^k, *J. Integer Sequences* Vol. 13 (2010), Article 10.5.4.

[11] Andrew D. Loveless, A congruence for products of binomial coefficients modulo a composite, *INTEGERS, Electronic Journal of Combinatorial Number Theory* Vol. 7 (2007), #A44, 1–9.

[12] F. Luca and P. T. Young, On the binary expansion of the odd Catalan numbers, *Aportaciones Matematicas, Investigacion* Vol. 20 (2011), 185–190.

[13] G. Xin and J-F. Xu, A short approach to Catalan numbers modulo 2^r, *Electronic Journal of Combinatorics* Vol. 18 (2011), #P177, 1–12.