Journal of Integer Sequences, Vol. 13 (2010),
Article 10.5.4

Catalan Numbers Modulo 2^k

Shu-Chung Liu[1]
Department of Applied Mathematics
National Hsinchu University of Education
Hsinchu, Taiwan
liularry@mail.nhcue.edu.tw

and

Jean C.-C. Yeh
Department of Mathematics
Texas A & M University
College Station, TX 77843-3368
USA

Abstract

In this paper, we develop a systematic tool to calculate the congruences of some combinatorial numbers involving $n!$. Using this tool, we re-prove Kummer's and Lucas' theorems in a unique concept, and classify the congruences of the Catalan numbers c_n (mod 64). To achieve the second goal, c_n (mod 8) and c_n (mod 16) are also classified. Through the approach of these three congruence problems, we develop several general properties. For instance, a general formula with powers of 2 and 5 can evaluate c_n (mod 2^k) for any k. An equivalence $c_n \equiv_{2^k} c_{\bar{n}}$ is derived, where $\bar{n}$ is the number obtained by partially truncating some runs of 1 and runs of 0 in the binary string $[n]_2$. By this equivalence relation, we show that not every number in $[0, 2^k - 1]$ turns out to be a residue of c_n (mod 2^k) for $k \geq 2$.

1 Introduction

Throughout this paper, p is a prime number and k is a positive integer. We are interested in enumerating the congruences of various combinatorial numbers modulo a prime power

[1]Partially supported by NSC96-2115-M-134-003-MY2

$q := p^k$, and one of the goals of this paper is to classify Catalan numbers c_n modulo 64. For a prime modulus p, previous studies can be traced back to the famous Pascal's fractal formed by the parities of binomial coefficients $\binom{n}{k}$ (see for example [22]). As a pioneer in this problem, Kummer formulated the maximum power of p dividing $\binom{n}{k}$ [14, see also Theorem 2.4]. Lucas, another early researcher, developed the very useful calculating formula $\binom{n}{k} \equiv_p \prod_i \binom{n_i}{r_i}$, where "$\equiv_p$" denotes the equivalence of congruence modulo p; and each n_i (similarly for each r_i) is obtained from $[n]_p := \langle n_s \cdots n_1 n_0 \rangle_p$ denoting the sequence of digits representing n in the base-p system [17, or see Theorem 2.5]. A generalization of Lucas' Theorem for a prime power was established by Davis and Webb [2]. The classical problem of Pascal's triangle also has versions for modulus 4 and modulus 8 [3, 13]. The behavior of Pascal's triangle modulo higher powers of p is more complicated. Some rules of the behavior are discussed by Granville [12]. The reader can also refer to [11] for a survey of binomial coefficients modulo prime powers.

Several other combinatorial numbers have been studied for their congruences, for example, Apéry numbers [10, 18], Central Delannoy numbers [7] and weighted Catalan numbers [19].

The *p-adic order* of a positive integer n is denoted and defined as

$$\omega_p(n) := \max\{\alpha \in \mathbb{N} : p^\alpha | n\}.$$

We also use $p^\alpha \| n$ to denote the property that $p^\alpha | n$ but $p^{\alpha+1} \nmid n$. The *cofactor of n with respect to $p^{\omega_p(n)}$*, which is denoted and defined as

$$CF_p(n) := \frac{n}{p^{\omega_p(n)}},$$

is an important object in this paper. We also call $CF_p(n)$ the (*maximal*) *p-free factor* of n. The value ω_p indicates the divisibility by powers of p, which can be found in many previous studies (see for example [5]). However, the studies on CF_p was a little bit rare before. One of formulae about CF_p is that

$$CF_p(\binom{m}{n}) \equiv_p (-1)^{\omega_p(\binom{m}{n})} \prod_{i \geq 0} \frac{m_i!}{n_i! r_i!}, \tag{1}$$

where $r = m - n$. This formula was found by each of Anton (1869), Stickelberger (1890) and Hensel (1902). A generalized formula of (1) for modulus p^k can be found in [11]. Recently, Eu, Liu and Yeh used CF_p to enumerate the congruences of Catalan numbers and Motzkin number modulo 4 and 8 [8]. Note that this cofactor was denoted by $NF_p(n)$ in their paper.

Given a product $\prod_{i=1}^a M_i$ of integers M_i, clearly $\omega_p(\prod_{i=1}^a M_i) = \sum_{i=1}^a \omega_p(M_i)$ and usually it is easy to calculate; but $CF_p(\prod_{i=1}^a M_i) \pmod q$ is more difficult to evaluate. However, q and $CF_p(M_i)$ are coprime; so instead of considering the arithmetics in the ring $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$, we shall narrow our attention to the *modulo multiplication group* $\mathbb{Z}_q^* := \{t \in \mathbb{Z}_q \mid (t, q) = 1\}$. To evaluate $CF_p \pmod q$, Eu, Liu and Yeh [8] recently introduced a new index $E_{q,t}$, the *t-encounter function of modulus q*, with respect to a product $\prod_{i=1}^a M_i$ is denoted and defined as

$$E_{q,t}(\prod_{i=1}^a M_i) := \sum_{i=1}^a \chi(CF_p(M_i) \equiv_q t),$$

where χ is the Boolean function. If $\omega_p(\prod_{i=1}^a M_i) \geq k$, then $\prod_{i=1}^a M_i \equiv_q 0$; otherwise

$$\prod_{i=1}^{a} M_i \equiv_q p^{\omega_p(\prod_{i=1}^a M_i)} \prod_{t\in\mathbb{Z}_q^*} t^{\,E_{q,t}(\prod_{i=1}^a M_i)}. \tag{2}$$

The evaluation of $\prod_{t\in\mathbb{Z}_q^*} t^{\,E_{q,t}(\prod_{i=1}^a M_i)}$ shall be operated in $\mathbb{Z}_q^*$. Alternatively and more efficiently,

$$\prod_{i=1}^{a} M_i \equiv_q p^{\omega_p(\prod_{i=1}^a M_i)} \prod_{t\in\mathbb{Z}_{q'}^*} t^{\,E_{q',t}(\prod_{i=1}^a M_i)}, \tag{3}$$

where $q' = p^{k'}$ with some k' such that $k - \omega_p(\prod_{i=1}^a M_i) \leq k' \leq k$.

Many combinatorial numbers are in form of quotient $\prod_{i=1}^a M_i / \prod_{j=1}^b N_j$. By analogy, let us define

$$E_{q,t}\Big(\frac{\prod_{i=1}^a M_i}{\prod_{j=1}^b N_j}\Big) := E_{q,t}\Big(\prod_{i=1}^{a} M_i\Big) - E_{q,t}\Big(\prod_{j=1}^{b} N_j\Big),$$

and then

$$\frac{\prod_{i=1}^a M_i}{\prod_{j=1}^b N_j} \equiv_q p^{\omega_p(\prod_{i=1}^a M_i) - \omega_p(\prod_{j=1}^b N_j)} \prod_{t\in\mathbb{Z}_q^*} t^{\,E_{q,t}(\frac{\prod_{i=1}^a M_i}{\prod_{j=1}^b N_j})}. \tag{4}$$

In this paper, we first investigate the most primitive product, namely the factorial $n!$, and then study the Catalan number $c_n := \frac{(2n)!}{(n+1)(n!)^2}$. By enumerating ω_2 and $E_{q,t}$ for $q = 4$ and 8, Eu, Liu and Yeh characterized the congruences of Catalan numbers and Motzkin numbers modulo 4 and 8 [8]. Here we improve their calculating techniques and challenge higher moduli up to 64.

It is well known that $\mathbb{Z}_{2^k}^*$ is isomorphic to $C_2 \times C_{2^{k-2}}$ $(k \geq 2)$, and the group $\mathbb{Z}_{p^k}^*$ is cyclic for any odd prime p. A breakthrough of our work is that by transforming the multiplicative group $\mathbb{Z}_n^*$ to the corresponding additive group and fitting $\prod_{t\in\mathbb{Z}_q^*} t^{\,E_{q,t}(\prod_{i=1}^a M_i)}$ into an admissible additive process, we can develop efficient and powerful formulae for enumerating the congruences of many combinatorial numbers. With this new tool, the time-consuming methods in [8] become easy applications.

We not only work for moduli 8, 16 and 64, but also develop several general properties. In Theorem 4.4, we derive that $c_n \pmod{2^k}$ is equivalent to the multiple of certain powers of 2 and 5. In Corollaries 4.3, 4.5 and 5.4, we derive three easy formulae for $c_n \pmod{2^k}$ in case that $\omega_2(c_n) = k - d$ for $d = 1, 2, 3$ respectively. In addition, Theorems 5.1 and 5.2 provide two rough classifications for $CF_2(n!)$ and $c_n \pmod{2^k}$ respectively. The second classification offers a shortcut to enumerate $c_n \pmod{2^k}$ when n is very large. It also implies Theorem 5.3, which claims that not every number in $[0, 2^k - 1]$ admits to be a congruence of $c_n \pmod{2^k}$ for $k \geq 2$.

The paper is organized as follows. In Section 2, the tools CF_2 and $E_{2^k,t}$, introduced by Eu, Liu and Yeh [8], are generalized to work for any prime p, and then we re-prove Kummer's and Lucas' Theorems using a unique idea—the concept of ω_p and $E_{q,t}$. An isomorphism T_q from the multiplicative group $\mathbb{Z}_{p^k}^*$ to an additive group is introduced in Section 3. Some results for $T_{2^k}(CF_2(n!))$ and $T_{2^k}(CF_2(c_n))$ are given there. In Sections 4, 5 and 6, we study the congruences of c_n with moduli 8 (re-proving the result in [8]), 16 and 64, respectively. Several comments for further research are given in Section 7, the final section.

2 $\omega_p(n!)$ and $E_{q,t}(n!)$; Borrows and Carries

Recall the p-adic order ω_p and t-encounter function $E_{q,t}$ defined in the previous section. Since the factorial $n!$ is the most elementary piece in the formulae of various combinatorial numbers, it is crucial to investigate $\omega_p(n!)$ and $E_{q,t}(n!)$. The first lemma of this section is generalized from the two similar lemmas in [8]. Before giving that lemma, we need some new notation.

Let $[a, b] := \{a, a+1, \ldots, b\}$ for two integers a and b, where $a \leq b$. Additionally, let $[a, b]_{\mathrm{o}}$ contain all odd numbers in $[a, b]$. Given a positive integer n, which is normally represented by a decimal expansion using Arabic numerals $0, 1, \ldots, 9$, we want to transform it into a base-p expansion using *digits* $0, 1, \ldots, p-1$. Such an expansion is denoted as a sequence of digits

$$[n]_p := \langle n_r n_{r-1} \cdots n_1 n_0 \rangle_p,$$

provided $p^r \leq n < p^{r+1}$ for some $r \in \mathbb{N}$ and $n = n_r p^r + n_{r-1} p^{r-1} + \cdots + n_1 p + n_0$ with $n_i \in [0, p-1]$, where n_i is called the *i-th place digit* of $[n]_p$ (or of n). For convenience, we also let $n_{r+1} = n_{r+2} = \cdots = 0$, but formally these 0's of higher places do not belong to the sequence $[n]_p$. We can even define $[0]_p$ as an empty sequence. Reversely, we define

$$|\langle n_r n_{r-1} \cdots n_1 n_0 \rangle_p| := n_r p^r + n_{r-1} p^{r-1} + \cdots + n_1 p + n_0 = n.$$

Let $d_s(n) := \sum_{i \geq s} n_i$ which is the *digit sum* starting from the s-th place. We simply let $d(n) = d_0(n)$, called the *total digit sum*.

Lemma 2.1. *Let $q = p^k$, $t \in \mathbb{Z}_q^*$ and $[n]_p = \langle n_r n_{r-1} \ldots n_1 n_0 \rangle_p$. The p-adic order $\omega_p(n!)$ and t-encounter function $E_{q,t}(n!)$ are evaluated as follows:*

$$\begin{aligned} \omega_p(n!) &= \frac{n - d(n)}{p-1}, & (5) \\ E_{q,t}(n!) &= \frac{|\langle n_r \cdots n_k n_{k-1} \rangle_p| - d_{k-1}(n)}{p-1} + \sum_{i \geq 0} \chi(|\langle n_{i+k-1} \cdots n_{i+1} n_i \rangle_p| \geq t). & (6) \end{aligned}$$

Proof. We have

$$\begin{aligned} \omega_p(n!) &= \sum_{k=1}^{s} \lfloor n/p^k \rfloor \\ &= |\langle n_r n_{r-1} \ldots n_2 n_1 \rangle_p| + |\langle n_r n_{r-1} \ldots n_2 \rangle_p| + \cdots + |\langle n_r \rangle_p|, \end{aligned}$$

because $\lfloor n/p^k \rfloor$ counts the number of integers in $[1, n]$ that are multiples of p^k. From this equation, the total contribution to $\omega_p(n!)$ caused by n_k is $(p^{k-1} + p^{k-2} + \cdots + 1) n_k$. Thus, $\omega_p(n!) = \sum_{k=1}^{s} \frac{(p^k-1)}{p-1} n_k = \sum_{k=0}^{s} \frac{(p^k-1)}{p-1} n_k = \frac{n-d(n)}{p-1}$ and the proof of the first equation follows.

The concept for the proof of the second equation is similar. For those $m \in [1, n]$ with the same order $\omega_p(m) = i$, the sum of their $\chi(m/p^i \equiv_q t)$ equals $\left\lfloor (\lfloor \frac{n}{p^i} \rfloor + (q-t))/q \right\rfloor$. We add $q - t$ into the numerator because the terms occurring of congruence t are, from 1 to n, the t-th, $(t+q)$-th, $(t+2q)$-th, etc. Therefore, we have

$$\begin{aligned}
E_{q,t}(n!) &= \sum_{i\geq 0} \left\lfloor \frac{\lfloor \frac{n}{p^i} \rfloor + (q-t)}{q} \right\rfloor & (7)\\
&= \sum_{i\geq k-1} \frac{(p^{i-k+1}-1)n_i}{p-1} + \sum_{i\geq 0} \chi(|\langle n_{i+k-1}\cdots n_{i+1}n_i\rangle_p| \geq t) & (8)\\
&= \frac{|\langle n_r \cdots n_k n_{k-1}\rangle_p| - d_{k-1}(n)}{p-1} + \sum_{i\geq 0} \chi(|\langle n_{i+k-1}\cdots n_{i+1}n_i\rangle_p| \geq t),
\end{aligned}$$

where the second summation in (8) counts the effect of the floor function caused by $q - t$ in (7), while the first summation is obtained by ignoring $q - t$. ∎

Note that equation (5) is the Legendre formula. For convenience, we shall evaluate the two terms in (6) separately. Let $E_{q,t}(n!) := E'_q(n!) + E''_{q,t}(n!)$ by defining

$$\begin{aligned}
E'_q(n!) &:= \frac{|\langle n_r \cdots n_{k-1}\rangle_p| - d_{k-1}(n)}{p-1}, \text{ and} & (9)\\
E''_{q,t}(n!) &:= \sum_{i\geq 0} \chi(|\langle n_{i+k-1}\cdots n_{i+1}n_i\rangle_p| \geq t). & (10)
\end{aligned}$$

Also note that the digit n_{k-1} actually does not affect the value of $E'_q(n!)$. It is the same as for n_0 to $\omega_p(n!)$.

The products $(m+n)!$ and $(m-n)!$ also occur frequently in the formulae of various combinatorial numbers. To apply Lemmas 2.1 directly, we have to realize every digit in $[m+n]_p$ and $[m-n]_p$. Can we simply rely on the digits in $[m]_p$ and $[n]_p$ without operating summation $m+n$ and subtraction $m-n$ completely? We fulfill this idea in the following.

Given nonnegative integers $m \geq n$ and $i \geq j$, let us define

$$\begin{aligned}
\beta_p^+(m,n;i,j) &:= \chi(|\langle m_i m_{i-1}\cdots m_j\rangle_p| + |\langle n_i n_{i-1}\cdots n_j\rangle_p| \geq p^{i-j+1}),\\
\beta_p^-(m,n;i,j) &:= \chi(|\langle m_i m_{i-1}\cdots m_j\rangle_p| < |\langle n_i n_{i-1}\cdots n_j\rangle_p|),
\end{aligned}$$

and briefly let $\beta_p^+(m,n;i) := \beta_p^+(m,n;i,0)$ and $\beta_p^-(m,n;i) := \beta_p^-(m,n;i,0)$, which indicate respectively the possible *carry* and *borrow* transmitting between the i-th and the $(i+1)$-st places when we operate summation $m+n$ and subtraction $m-n$ in the base-p system. Define

$$\begin{aligned}
C_p(m,n) &:= \sum_{i\geq 0} \beta_p^+(m,n;i) \text{ and}\\
B_p(m,n) &:= \sum_{i\geq 0} \beta_p^-(m,n;i),
\end{aligned}$$

which are respectively the numbers of *total carries* for (operating) $m+n$ and *total borrows* for $m-n$.

Lemma 2.2. *Let $m, n, i \in \mathbb{N}$ with $m \geq n$. In the base-p system, we have*

$$\begin{aligned} d(m+n) &= d(m) + d(n) - (p-1)C_p(m,n) \text{ and} \\ d(m-n) &= d(m) - d(n) + (p-1)B_p(m,n). \end{aligned}$$

Proof. Let us observe the "net contribution" to $d(m+n)$ made by the two i-th place digits in $[m]_p$ and $[n]_p$, when operating $m+n$ in the base-p system. We claim that this net contribution is

$$m_i + n_i - \beta_p^+(m,n;i)(p-1).$$

The first equation of the lemma directly follows this claim.

If no carry occurs at the i-th place, then $(m+n)_i = m_i + n_i + \beta_p^+(m,n;i-1)$. So $(m+n)_i$ (as well as the digit sum $d(m+n)$) simply obtains net contribution $m_i + n_i$ from these two digits. Note that $\beta_p^+(m,n;i-1)$ may increase $(m+n)_i$; however, as for "net contribution" it has been counted at the $(i-1)$-st place. If a carry occurs, both $(m+n)_i$ and $(m+n)_{i+1}$ are effected, while $(m+n)_i$ turns to be $m_i + n_i + \beta_p^+(m,n;i-1) - p$ and $(m+n)_{i+1}$ obtains an extra $1 = \beta_p^+(m,n;i)$. Thus, the net contribution to $d(m+n)$ causing by m_i and n_i is then $m_i + n_i - p + 1$. So the claim follows.

By a similar way, we can explain why $(p-1)B_p(m,n)$ must be added into the second equation. ∎

Now applying Lemmas 2.1 and 2.2, we obtain the following result.

Lemma 2.3. *Let $n \geq n$ and suppose $[m]_p = \langle \ldots m_1 m_0 \rangle_p$ and $[n]_p = \langle \ldots n_1 n_0 \rangle_p$. Than*

$$\begin{aligned} \omega_p((m+n)!) &= \frac{m+n-d(m)-d(n)}{p-1} + C_p(m,n) \text{ and} \\ \omega_p((m-n)!) &= \frac{m-n-d(m)+d(n)}{p-1} - B_p(m,n). \end{aligned}$$

Both $E_{q,t}((m+n)!)$ and $E_{q,t}((m-n)!)$ are useful, but not in this paper; so we skip them here. Before ending this section, we use ω_p and $E_{q,t}$ to re-prove the following two famous and useful theorems.

Theorem 2.4 (Kummer, 1852 [14]). *Let p be a prime and $m, n \in \mathbb{N}$ with $m \geq n$. Then we have*

$$\begin{aligned} \omega_p(\binom{m+n}{m}) &= C_p(m,n) \text{ and} \\ \omega_p(\binom{m}{n}) &= B_p(m,n). \end{aligned}$$

Proof. By Lemmas 2.1 and 2.3, we derive

$$\begin{aligned} \omega_p(\binom{m+n}{m}) &= \omega_p((m+n)!) - \omega_p(m!) - \omega_p(n!) \\ &= \left[\frac{m+n-d(m)-d(n)}{p-1} + C_p(m,n)\right] - \frac{m-d(m)}{p-1} - \frac{n-d(n)}{p-1} \\ &= C_p(m,n). \end{aligned}$$

The proof for $\omega_p(\binom{m}{n})$ is similar. ■

Theorem 2.5 (Lucas, 1877 [17]). *The binomial coefficient modulo a prime p can be computed as follows*

$$\binom{m}{n} \equiv_p \prod_{i\geq 0} \binom{m_i}{n_i},$$

where $\langle \cdots m_1 m_0 \rangle_p$ and $\langle \cdots n_1 n_0 \rangle_p$ are the expansions of m and n in the base-p system, respectively.

Proof. We may assume that $m_i \geq n_i$ for all i. Because $m_i < n_i$ means that a borrow occurs and then $p|\binom{m}{n}$ by Kummer's Theorem. Also $\binom{m_i}{n_i} = 0$ is due to $m_i < n_i$. So the stated equivalence holds. By assumption, we have $\omega_p(\binom{m}{n}) = 0$ and $(m-n)_i = m_i - n_i$. Now applying (4), we see

$$\begin{aligned}
\binom{m}{n} &\equiv_p \prod_{t\in[1,p-1]} t^{E_{p,t}(m!)-E_{p,t}(n!)-E_{p,t}((m-n)!)} \\
&= \prod_{t\in[1,p-1]} t^{\sum_{i\geq 0}[\chi(m_i\geq t)-\chi(n_i\geq t)-\chi((m-n)_i\geq t)]} && (11)\\
&= \prod_{i\geq 0}\prod_{t\in[1,p-1]} t^{\chi(m_i\geq t)-\chi(n_i\geq t)-\chi(m_i-n_i\geq t)} \\
&= \prod_{i\geq 0} t^{E_{p,t}(m_i!)-E_{p,t}(n_i!)-E_{p,t}((m_i-n_i)!)} && (12)\\
&\equiv_p \prod_{i\geq 0}\binom{m_i}{n_i}.
\end{aligned}$$

Among these equivalences and equations, both (11) and (12) are due to Lemma 2.1 and three $E'(\cdot)$ canceling each other; the last equivalence is because there is no borrow. ■

The reader can also find a very neat proof of Lucas' Theorem in [9]. That proof is based on the Binomial Expansion Theorem and a simple fact that $p|\binom{p}{r}$ for a prime p and $r = 1, 2, \ldots, p-1$. Another kind of proof uses induction to substitute the Binomial Expansion Theorem. In contrast, our new proof requires neither. Even more appealing is that our new proofs of Kummer's and Lucas' Theorems are united in a single idea—the concept of ω_p and $E_{p,t}$.

3 Transforming $\mathbb{Z}_q^*$ to an additive group

For performing the power of t and the product $\prod$ appearing in $CF_p(n!) \equiv_q \prod_{t\in\mathbb{Z}_q^*} t^{E_{q,t}(n!)}$, we need to work on the domain $(\mathbb{Z}_q^*, \times_q)$ (modulo multiplication group). But operating $\times_q$ is complicated. We simplify this cumbersome operation by transforming $(\mathbb{Z}_q^*, \times_q)$ to an additive group under isomorphism as follows:

$$\begin{aligned}
(\mathbb{Z}_{2^k}^*, \times_q) &\cong (C_2 \times C_{2^{k-2}}, +) \quad \text{for } k \geq 2; && (13)\\
(\mathbb{Z}_{p^k}^*, \times_q) &\cong (C_{p^{k-1}(p-1)}, +) \quad \text{for an odd prime } p, && (14)
\end{aligned}$$

Table 1: The first few example for the isomorphisms $(\mathbb{Z}^*_{2^k}, \times_q) \cong (C_2 \times C_{2^{k-2}}, +)$

	0	1
0	1	5
1	3	7

	0	1	2	3
0	1	5	9	13
1	7	3	15	11

	0	1	2	3	4	5	6	7
0	1	5	25	29	17	21	9	13
1	15	11	23	19	31	27	7	3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	5	25	61	49	53	9	45	33	37	57	29	17	21	41	13
1	31	27	7	35	47	43	23	51	63	59	39	3	15	11	55	19

where C_m represents a cyclic group of order m. Please, refer to [20] and also see example in Table 1 as $q = 8, 16, 32, 64$.

In the rest of the paper, we focus only on $p = 2$. To limit the length of this paper, we will collect the results for an odd prime power modulus in a more extensive paper in the future.

The multiplication in $(\mathbb{Z}^*_q, \times_q)$ is then easily carried out through the corresponding addition in $(C_2 \times C_{2^{k-2}}, +)$. For instance,

$$\begin{aligned}
7^5 \times_{16} 11^{15} &\equiv_{16} {T_{16}}^{-1}(5\, T_{16}(7) + 15\, T_{16}(11)) \\
&\equiv_{16} {T_{16}}^{-1}(5\,(1,0) + 15\,(1,3)) \\
&\equiv_{16} {T_{16}}^{-1}((1,0) + (1,1)) \\
&\equiv_{16} {T_{16}}^{-1}((0,1)) \\
&\equiv_{16} 5,
\end{aligned}$$

where T_{16} is the isomorphism from $\mathbb{Z}^*_{16}$ to $C_2 \times C_4$ demonstrated in Table 1.

Let $q = 2^k$. The isomorphism

$$T_q : (\mathbb{Z}^*_q, \times_q) \to (C_2 \times C_{q/4}, +) \text{ for } k \geq 2,$$

is constructed as follows. We use $\mathbf{x}$ or (b, u) to denote an element of $C_2 \times C_{q/4}$, and define $T_q(t) := \mathbf{x}(t) = (b(t), u_q(t))$. As notation, $b(t)$ has no subscript q for a reason that will be explained latter. The most trivial case is T_4 such that $b(1) = 0$, $b(3) = 1$ and $u_4(t) \equiv 0$, a constant function.

We assume $k \geq 3$ in this paragraph only. Define $\mathbb{Z}^{*,1}_q := \{t \in \mathbb{Z}^*_q \mid t \equiv_4 1\}$ and $\mathbb{Z}^{*,3}_q := \{t \in \mathbb{Z}^*_q \mid t \equiv_4 3\}$. Clearly, $\mathbb{Z}^{*,1}_q$ is a subgroup of $\mathbb{Z}^*_q$ and $\mathbb{Z}^{*,3}_q$ is the unique coset. It is also easy to prove by induction that $[5^{(2^{k-2})}]_2 = \langle \cdots 1 \underbrace{0 \cdots 0}_{k-1 \text{ zeros}} 1\rangle_2 \equiv_{2^k} 1$ and $\mathbb{Z}^{*,1}_q$ is a cyclic group with 5 as a generator. Therefore, we can make

$$\begin{aligned}
T_q(\mathbb{Z}^{*,1}_q) &= \{(0, u) \mid u \in C_{q/4}\} \text{ with } T_q(5) = (0, 1), \text{ and} \\
T_q(\mathbb{Z}^{*,3}_q) &= \{(1, u) \mid u \in C_{q/4}\}.
\end{aligned}$$

The reason of no subscript q for $b(t)$ is now clear, because we must have

$$b(t) = \left\{ \begin{array}{ll} 0 & \text{if } t \equiv_4 1 \\ 1 & \text{if } t \equiv_4 3 \end{array} \right\} = t_1 \quad \text{where } [t]_2 = \langle \cdots t_2 t_1 1 \rangle_2, \tag{15}$$

which is independent on q. The isomorphism $u_q : \mathbb{Z}_q^{*,1} \to C_{q/4}$ is now well defined by $u_q(5) = 1$. Precisely, $u_q(t)$ equals the minimal nonnegative integer u such that $5^u \equiv_q t$. As for those $t \in \mathbb{Z}_q^{*,3}$, let $\hat{t} \in \mathbb{Z}_q^{*,1}$ be the unique element satisfying $t + \hat{t} \equiv_q q/2$ and then define $u_q(t) := u_q(\hat{t})$. We leave the check that T_q is really an isomorphism to the reader.

Let us extend the domain of u_q from $\mathbb{Z}_q^*$ to $\mathbb{Z}_{\mathrm{o}}$, the set of odd integers, by simply defining $u_q(t) := u_q(t \pmod q)$ for any odd integer t. The following are three fundamental formulae about u_q.

Lemma 3.1. *Given integers $k' > k \geq 2$ and $q' := 2^{k'}, q := 2^k$, we have*

$$\begin{array}{llcll} u_{q'}(t) & (\mathrm{mod}\ \frac{q}{4}) & = & u_q(t) & \textit{for any } t \equiv_4 1; \\ u_{q'}(t) & (\mathrm{mod}\ \frac{q}{8}) & = & u_q(t) \quad (\mathrm{mod}\ \frac{q}{8}) & \textit{for any } t \equiv_4 3 \textit{ and } k \geq 3; \\ u_{q'}(t) & (\mathrm{mod}\ \frac{q}{4}) & = & u_q(t) + \frac{q}{8}\chi & \textit{for any } t \equiv_4 3 \textit{ and } k \geq 3, \end{array}$$

where χ is either 0 or 1.

Proof. The assertion can be more general by plugging two odd integers $t', t \in \mathbb{Z}_{\mathrm{o}}$ with $t' \equiv_q t$ into the both sides of each equation respectively. In case that $t', t \equiv_4 1$, by definition $5^{u_{q'}(t')} \equiv_{q'} t' \equiv_q t \equiv_q 5^{u_q(t)}$ or $5^{u_{q'}(t')} \equiv_q 5^{u_q(t)}$ in short. Since 5 is a generator of $\mathbb{Z}_q^{*,1}$ with order $\frac{q}{4}$. Thus, $u_{q'}(t') \equiv_{q/4} u_q(t)$ and the first equation (not equivalence) holds because $u_q(t) \in [0, \frac{q}{4} - 1]$.

Suppose $t' \equiv_q t$ and both $t', t \equiv_4 3$. We find the two numbers $\hat{t}', \hat{t} \equiv_4 1$ with $\hat{t}' \equiv_{q'} \frac{q'}{2} - t'$ and $\hat{t} \equiv_q \frac{q}{2} - t$, so that $u_{q'}(t') := u_{q'}(\hat{t}')$ and $u_q(t) := u_q(\hat{t})$ by definition. Clearly, $\hat{t}' \equiv_{q/2} \hat{t}$; so we can plug these two respectively into the both sides of the first equation of the lemma. Thus, we get $u_{q'}(\hat{t}') \pmod{\frac{q}{8}} = u_{q/2}(\hat{t})$ and then reach the general version of the second equation of the lemma as follows

$$u_{q'}(t') \quad (\mathrm{mod}\ \frac{q}{8}) = u_{q/2}(t) = u_q(t) \quad (\mathrm{mod}\ \frac{q}{8}),$$

where the second equation is a special case of the first one provided that $t' = t$ and $q' = q$.

The last equation of the lemma is a direct result of the second one. ■

Directly from Table 1, we have

$$\begin{array}{rcl} u_8(t) & = & t_2, \text{ and} \\ u_{16}(t) & = & t_1 + t_2 + 2t_3 - 2t_1 t_2. \end{array} \tag{16}$$

The greater the power $q = 2^k$, the more complicated $u_q(t)$ is. Comparing with the complication of the second entry in $T_q(t) = (b(t), u_q(t))$, the inverse T_q^{-1} is much easier to describe as follows:

$$T_q^{-1}(b, u) \equiv_q \left\{ \begin{array}{ll} 5^u & \text{if } b = 0 \\ 2^{k-1} - 5^u & \text{if } b = 1 \end{array} \right\} \equiv_q 2^{k-1} b + (-1)^b 5^u \quad \text{for } k \geq 2. \tag{17}$$

$T_{2^k}(CF_2(n!))$ and $T_{2^k}(CF_2(c_n))$

The argument in this subsection will show a difference in $T_{p^k}(CF_p(\cdot))$ between the cases $p = 2$ and p being an odd prime. This is another reason why we divide our discussion into two papers.

Let us extend the domain of u_q from $\mathbb{Z}_q^*$ to the set of odd integers, by simply define $u_q(t) := u_q(t \pmod q)$. In general, we have

$$\begin{aligned} T_q(CF_2(\prod_{i=1}^{a} M_i)) &= \sum_{t\in\mathbb{Z}_q^*} E_{q,t}(\prod_{i=1}^{a} M_i)\, T_q(t) && (18)\\ &= \sum_{\mathbf{x}\in C_2\times C_{q/4}} E_{q,{T_q}^{-1}(\mathbf{x})}(\prod_{i=1}^{a} M_i)\, \mathbf{x}. && (19)\end{aligned}$$

Any term of $E_{q,t}(\prod_{i=1}^{a} M_i)$ that is independent on t finally contributes $(0,0)$ in total to the above summation due to a simple algebraic property as follows:

$$\sum_{\mathbf{x}\in C_2\times C_{q/4}} \mathbf{x} = |C_{q/4}| \sum_{b\in C_2}(b,0) + |C_2| \sum_{u\in C_{q/4}} (0,u) = 2^{k-2}(1,0) + 2\,(0,2^{k-3}) = (0,0), \qquad (20)$$

when $k \geq 3$. A corresponding property is that

$$\prod_{t\in\mathbb{Z}_{2^k}^*} t = 1 \quad \text{for } k \geq 3 \text{ or } k = 1. \qquad (21)$$

By Lemma 2.1, the partial term $E'_q(n!)$ is independent on t; so we have $\sum_{\mathbf{x}\in C_2\times C_{q/4}} E'_q(n!)\,\mathbf{x} = (0,0)$ and we can ignore $E'_q(n!)$. Thus, if the formal product is $n!$, we improve (18) by a better formula as follows:

$$T_q(CF_p(n!)) = (b(CF_p(n!), u_q(CF_p(n!)) = \sum_{t\in\mathbb{Z}_q^*} E''_{q,t}(n!)\,(b(t), u_q(t)). \qquad (22)$$

However, the property (21) fails when $k = 2$ or p is an odd prime; so (22) does not work in this condition.

As for $k = 2$, not only the isomorphism $\mathbb{Z}_4^* \cong C_2$ is trivial, but also

$$CF_2(n!) \equiv_4 (-1)^{E_{4,3}(n!)} = (-1)^{r(n)+n_0+n_1} = (-1)^{d_2(n)+c_2(n)}, \qquad (23)$$

shown by Lemma 2.1 in [8], is a easy formula. Apart from n_0, n_1 and d_2, we have not defined some new notation in (23) yet. Over the sequence $[n]_2$, let $r(n)$ be the number of runs of 1, and let $c_2(n) := \sum_{i\geq 0} \chi(n_i = n_{i+1} = 1)$, i.e., the number of the consecutive pairs of 1. The last equality in (23) is due to the simple fact that $c_2(n) = d(n) - r(n)$. By (15) and (23), we conclude that

$$b(CF_2(n!)) \equiv_2 r(n) + n_0 + n_1 \equiv_2 d_2(n) + c_2(n) \equiv_2 zr(n) + n_1. \qquad (24)$$

The last equivalence will be explained later in (28).

In the following three sections, we develop formulae of $T_q(CF_p(n!))$ for $q = 8, 16, 32$ and 64, and also to evaluate the Catalan number, c_n, modulo 8, 16 and 64. (We skip 32.) The problem of $c_n \pmod 2$ can be easily solved by Lucas' Theorem. For the problem of c_n (mod 4), please refer to [8].

4 $b(CF_2(n!))$ and $u_8(CF_2(n!))$; Catalan numbers modulo 8

Given a multi-subset $\mathcal{M}$ and a subset T of $\mathbb{Z}_q$, let $\#(\mathcal{M}, T)$ be the number of elements (with multiplicity) in $\mathcal{M}$ belonging to T. Define a multi-set

$$\mathcal{S}_k(n) := \{|\langle n_{k+i-1} \ldots n_{i+1} n_i \rangle_2|\}_{i=0}^{r},$$

where $[n]_2 = \langle n_r \cdots n_1 n_0 \rangle_2$ and $\langle n_{k+i-1} \ldots n_{i+1} n_i \rangle_2$ is a *k-segment* contained in the sequence $\langle \overbrace{0 \cdots 00}^{k-1} n_r \cdots\ n_1 n_0 \rangle_2$. For example, given $[n]_2 = \langle 100110000101 \rangle_2$ we have $\mathcal{S}_3(n) := \{5, 2, 1, 0, 0, 4, 6, 3, 1, 4, 2, 1\}$ if we check all k-segments from right to left, and $\#(\mathcal{S}_3(n), \{3, 4\}) = 3$.

The following counting formulae for $\#(\mathcal{S}_3(n), \{t\})$ are easy to check.

$$\begin{aligned}
\#(\mathcal{S}_3(n), \{3\}) &= \sum_{i \geq 0} \chi(\langle n_{i+2} n_{i+1} n_i \rangle = \langle 011 \rangle) = r(n) - r_1(n); && (25)\\
\#(\mathcal{S}_3(n), \{4\}) &= \sum_{i \geq 0} \chi(\langle n_{i+2} n_{i+1} n_i \rangle = \langle 100 \rangle) = zr(n) - zr_1(n); && (26)\\
\#(\mathcal{S}_3(n), \{5\}) &= \sum_{i \geq 0} \chi(\langle n_{i+2} n_{i+1} n_i \rangle = \langle 101 \rangle) = zr_1(n) - n_1(1 - n_0);\\
\#(\mathcal{S}_3(n), \{6\}) &= \sum_{i \geq 0} \chi(\langle n_{i+2} n_{i+1} n_i \rangle = \langle 110 \rangle) = r(n) - r_1(n) - n_0 n_1,
\end{aligned}$$

where $r_1(n)$ is the number of isolated 1 in $[n]_2$, $zr(n)$ the number of runs made by 0, and $zr_1(n)$ the number of isolated 0. Referring to (10), (22) and Table 1 for $\mathbb{Z}_8^* \cong C_2 \times C_2$, we derive

$$\begin{aligned}
E''_{8,3}(n!)\,(1,0) &= (\sum_{i \geq 0} \chi(|\langle n_{i+2} n_{i+1} n_i \rangle_p| \geq 3), 0) = (\#(\mathcal{S}_3(n), \{3,4,5,6,7\}), 0),\\
E''_{8,5}(n!)\,(0,1) &= (0, \sum_{i \geq 0} \chi(|\langle n_{i+2} n_{i+1} n_i \rangle_p| \geq 5) = (0, \#(\mathcal{S}_3(n), \{5,6,7\})), \text{ and}\\
E''_{8,7}(n!)\,(1,1) &= \Big[\sum_{i \geq 0} \chi(|\langle n_{i+2} n_{i+1} n_i \rangle_p| \geq 7)\Big](1,1) = (\#(\mathcal{S}_3(n), \{7\}), \#(\mathcal{S}_3(n), \{7\})).
\end{aligned}$$

Summing up the above three, we obtain

$$\begin{aligned}
T_8(CF_2(n!)) &= (b(CF_2(n!)), u_8(CF_2(n!)))\\
&= (\#(\mathcal{S}_3(n), \{3,4,5,6\}), \#(\mathcal{S}_3(n), \{5,6\})) \pmod 2 && (27)\\
&= (zr(n) + n_1,\ r(n) + r_1(n) + zr_1(n) + n_1) \pmod 2 && (28)\\
&= (r(n) + n_0 + n_1,\ r(n) + r_1(n) + zr_1(n) + n_1) \pmod 2. && (29)
\end{aligned}$$

The last equation is due to the fact $r(n) = zr(n) + n_0$. This equation also explains the last equivalence in (24). Again we see the fact that $b(CF_2(n!))$ is independent on q.

In the rest of this section, we re-prove the following theorem, which was first shown in [8], through an easier approach.

Theorem 4.1 (Eu, Liu and Yeh, 2008 [8]). *Let c_n be the n-th Catalan number. Then $c_n \not\equiv_8 3, 7$ for any n. And for the other congruences, we have*

$$c_n \equiv_8 \begin{cases} 1 & \text{if} \quad n = 0 \text{ or } 1; \\ 2 & \text{if} \quad n = 2^a + 2^{a+1} - 1 \text{ for some } a \geq 0; \\ 4 & \text{if} \quad n = 2^a + 2^b + 2^c - 1 \text{ for some } c > b > a \geq 0; \\ 5 & \text{if} \quad n = 2^a - 1 \text{ for some } a \geq 2; \\ 6 & \text{if} \quad n = 2^a + 2^b - 1 \text{ for some } b - 2 \geq a \geq 0; \\ 0 & \text{otherwise.} \end{cases}$$

We first discuss some general properties for modulus $q = 2^k$. Since $c_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)(n!)^2}$, by Lemma 2.1 we have

$$\begin{aligned} \omega_2(c_n) &= [2n - d(2n)] - \omega_2(n+1) - 2[n - d(n)] \\ &= 2n - d(n) - \min\{i \mid n_i = 0\} - 2n + 2d(n) \\ &= d(n) - \min\{i \mid n_i = 0\} \\ &= d(n+1) - 1. \end{aligned}$$

The last equation is due to the fact that $\min\{i \mid n_i = 0\}$ is the length of the run of 1 starting at the 0-th place of $[n]_2$. In the process of proving Theorem 4.1, the above result for $\omega_2(c_n)$ provides a new proof of the next theorem.

Theorem 4.2 (Deutsch and Sagan, 2006 [4]). *For $n \in \mathbb{N}$ we have*

$$\omega_2(c_n) = d(n+1) - 1 = d(n) - \min\{i \mid n_i = 0\}.$$

When we deal with c_n modulo 2^k, this theorem suggests that $[n]_2$ be bisected into two particular segments as follows:

$$\langle \overbrace{10\cdots1100}^{\text{The rightmost is a 0.}} \underbrace{1\cdots1}_{\text{This segment of all 1 might be empty.}} \rangle_2 \tag{30}$$

We call these two segments the *principal segments* of $[n]_2$ and use $[2\alpha]_2$ and $\langle 1^\beta \rangle_2$ to denote them respectively, where $\alpha, \beta \in \mathbb{N}$ and 1^β means a string of 1 of length β. We use 2α because its 0-th place digit must be 0. Equivalently, we can also define

$$\begin{aligned} \alpha &:= \frac{CF_2(n+1) - 1}{2}, \text{ and} \\ \beta &:= \omega_2(n+1) = \min\{i \mid n_i = 0\}. \end{aligned}$$

Here we find that the notation α is good to use in the following property which directly follows Theorem 4.2.

Corollary 4.3. *In general, we have $\omega_2(c_n) = d(\alpha)$. In particular, $c_n \equiv_q 0$ if and only if $d(\alpha) \geq k$, and $c_n \equiv_q q/2$ if and only if $d(\alpha) = k - 1$.*

Due to this corollary, from now on we focus only on $d(\alpha) \le k-2$. Let us examine $T_8(CF_2(n!))$. Its first entry is enumerated by using (15) and (24) as follows:

$$\begin{aligned}
b(CF_2(c_n)) &\equiv_2 [zr(2n)+(2n)_1] - b(CF_2(n+1)) - 2[zr(n)+n_1] \\
&\equiv_2 [(zr(n)+n_0)+n_0] + b(2\alpha+1) \\
&\equiv_2 zr(n)+\alpha_0 \\
&\equiv_2 (zr(\alpha)+\alpha_0)+\alpha_0 \\
&\equiv_2 zr(\alpha).
\end{aligned} \tag{31}$$

Since $b(CF_2(c_n))$ is independent on q, this identity derives a general formula as follows.

Theorem 4.4. *Let $n \in \mathbb{N}$, $q = 2^k$ with $k \ge 2$, and $\alpha = (CF_2(n+1)-1)/2$. Then we have*

$$c_n \equiv_q (-1)^{zr(\alpha)} 2^{d(\alpha)} 5^{u_q(CF_2(c_n))}. \tag{32}$$

In particular, when $k = 2$ we have

$$c_n \equiv_4 (-1)^{zr(\alpha)} 2^{d(\alpha)}. \tag{33}$$

Proof. By (17), Theorem 4.2 (or Corollary 4.3) and the result of $b(CF_2(c_n))$ in (31), we have

$$\begin{aligned}
c_n &\equiv_q 2^{\omega_2(c_n)}\left[2^{k-1}b + (-1)^b 5^u\right] \\
&\equiv_q 2^{d(\alpha)}\left[2^{k-1}zr(\alpha) + (-1)^{zr(\alpha)} 5^{u_q(CF_2(c_n))}\right].
\end{aligned}$$

We finish the proof of the first assertion after considering two cases: $d(\alpha) = 0$ (which implies $zr(\alpha) = 0$) and $d(\alpha) \ge 1$. Notice that $u_4(t) = 0$ and then the second assertion follows. ■

The equivalence (33) is actually a rewrite of Eu, Liu and Yeh's result in [8]. The immediate consequence that $c_n \not\equiv_4 3$ was also given by them. The following two auxiliary corollaries directly follows Theorem 4.4.

Corollary 4.5. *Let $n, k \in \mathbb{N}$ with $k \ge 3$, $\alpha = (CF_2(n+1)-1)/2$ and $d(\alpha) = k-2$. We have*

$$c_n \equiv_q (-1)^{zr(\alpha)} \frac{q}{4}.$$

Corollary 4.6. *Let $n \in \mathbb{N}$ and $\alpha = (CF_2(n+1)-1)/2$. We have*

$$CF_2(c_n) \equiv_4 (-1)^{zr(\alpha)}.$$

Corollary 4.5 solves the case $d(\alpha) = k-2$ and is an improvement of Corollary 4.3. We will deal with the case $d(\alpha) = k-3$ by Corollary 5.4 in the next section.

Formula (32) offers a general method to enumerate $c_n \pmod{2^k}$, but it does not offer the classification like Theorem 4.1. On the other hand, Table 1 provides an easier way without calculating 5^{u_q} when k is small. We use the second way to classify c_n modulo 8, 16 and 64. However, the enumeration of $u_q(CF_2(c_n))$ is crucial through either way. The formula for $u_q(CF_2(c_n))$ of course depends on q and the large is k, the more complicated is it. Fortunately, what we need here is $u_8(CF_2(c_n))$ which is quit easy as follows:

$$\begin{aligned}
u_8(CF_2(c_n)) &\equiv_2 [r(2n)+r_1(2n)+zr_1(2n)+(2n)_1]-u_8(CF_2(n+1)) \qquad (34)\\
&\quad -2[r(n)+r_1(n)+zr_1(n)+n_1]\\
&\equiv_2 r(n)+r_1(n)+[zr_1(n)+n_0-n_1(1-n_0)]+n_0+u_8(2\alpha+1)\\
&= [r(\alpha)+\chi(\beta\geq 1)]+[r_1(\alpha)+\chi(\beta=1)]+[zr_1(\alpha)+\alpha_0-\alpha_1(1-\alpha_0)]\\
&\quad -[\chi(\beta\geq 2)+\chi(\alpha=1)\chi(\beta=0)]\chi(\beta=0)+\alpha_1\\
&\equiv_2 \chi(\beta\geq 2)+\chi(\alpha=1,\beta=0)+r(\alpha)+r_1(\alpha)+zr_1(\alpha)+\alpha_0(1-\alpha_1). \qquad (35)
\end{aligned}$$

By the formula of $u_8(CF_2(c_n))$, we can finish the mission of this section. Let us rewrite Theorem 4.1 in a new format using α and β as follows. The equivalence of these two theorems is easy to check.

Theorem 4.7. *Given $n\in\mathbb{N}$, let $\alpha=\frac{CF_2(n+1)-1}{2}$ and $\beta=\min\{i\mid n_i=0\}$. We have*

$$c_n \equiv_8 \begin{cases} \left.\begin{matrix}1\\5\end{matrix}\right\} & \text{if}\quad d(\alpha)=0 \text{ and } \quad \begin{cases}\beta=0 \text{ or } 1,\\ \beta\geq 2,\end{cases}\\ \left.\begin{matrix}2\\6\end{matrix}\right\} & \text{if}\quad d(\alpha)=1 \text{ and } \quad \begin{cases}\alpha=1,\\ \alpha\geq 2,\end{cases}\\ 4 & \text{if}\quad d(\alpha)=2,\\ 0 & \text{if}\quad d(\alpha)\geq 3.\end{cases}$$

Proof. The congruences 0, 2, 4 and 6 can be easily solved by Corollaries 4.3 and 4.5. The only remaining case is $d(\alpha)=0$. In this case, every term related to α turns to be 0 in (35). Then plug into (32) and obtain

$$c_n \equiv_8 (-1)^0 2^0 5^{\chi(\beta\geq 2)} \equiv_8 5^{\chi(\beta\geq 2)}.$$

Therefore, $c_n\equiv_8 1$ if and only if $[n]_2=\langle 1\rangle_2$ or it is an empty sequence, and $c_n\equiv_8 5$ if and only if $[n]_2=\langle 1^\beta\rangle_2$ for $\beta\geq 2$. The proof is complete now. ■

5 $u_{16}(CF_2(n!))$; Catalan numbers modulo 16

Since we already know $\omega(c_n)=d(\alpha)$ and $b(CF_2(c_n))=zr(\alpha)$, to enumerate $c_n \pmod q$ now relies on $u_q(CF_2(c_n))$, which depends on $u_q(CF_2(n!))$ further. Of course, directly dealing with modulus 64 will fill the unsolved gape for both moduli 16 and 32; however, when q is larger $u_q(CF_2(n!))$ becomes more complicated. In order to deal with modulus 64 smoothly, we consider solving the problem of $c_n \pmod{16}$ as a necessary practice and preparation.

First of all, we state a general formula of $u_q(CF_2(n!))$ for any $q=2^k$. By (10) and (22), we derive that

$$
\begin{aligned}
u_q(CF_2(n!)) &\equiv_{q/4} \sum_{t\in\mathbb{Z}_q^*} E''_{q,t}(n!)\, u_q(t) \\
&= \sum_{t\in\mathbb{Z}_q^*} \chi(|\langle n_{i+k-1}\cdots n_{i+1}n_i\rangle_2| \geq t)\, u_q(t) \\
&= \sum_{t\in\mathbb{Z}_q^*} \#(\mathcal{S}(n),[t,q-1])\, u_q(t) \\
&= \sum_{s\in[1,q-1]} \#(\mathcal{S}(n),\{s\}) \sum_{t\in[1,s]_{\mathrm{o}}} u_q(t) \qquad (36)\\
&= \sum_{s\in[3,q-2]} \#(\mathcal{S}(n),\{s\}) \sum_{t\in[3,s]_{\mathrm{o}}} u_q(t) \qquad (37)\\
&= \sum_{s\in[3,q-3]_{\mathrm{o}}} \#(\mathcal{S}(n),\{s,s+1\}) \sum_{t\in[3,s]_{\mathrm{o}}} u_q(t) \qquad (38)
\end{aligned}
$$

where $[1,s]_{\mathrm{o}}$ is the set of odd integers in $[1,s]$. Note that $\sum_{t\in[1,s]_{\mathrm{o}}} u_q(t) = \sum_{t\in[3,s]_{\mathrm{o}}} u_q(t)$ for $u_q(1)=0$. For this reason, we eliminate $s=1,2$ in the first summation of (36). Moreover, we eliminate $s=q-1$ because $\sum_{t\in[1,q-1]_{\mathrm{o}}} u_q(t)=0$ (see the second entry in (20)). The last formula (38) is because $\sum_{t\in[3,s]_{\mathrm{o}}} u_q(t) = \sum_{t\in[3,s+1]_{\mathrm{o}}} u_q(t)$ for any odd s.

Depending on k, there are several kinds of k-segments (we mean $[t]_2$ for $t\in[0,q-1]$) irrelevant to the counting in (37). For example, we see in (27) that $u_8(CF_2(n!))$ only counts on the 3-segments $[5]_2$ and $[6]_2$ appearing in $[n]_2$, and it is irrelevant to the other 3-segments. However, we shall only focus on the two kinds of k-segments of irrelevance that are independent on k, i.e., $[0]_2=\langle 0^k\rangle_2$ and $[q-1]_2=\langle 1^k\rangle_2$. Because of the irrelevancy of these two kinds of k-segments appearing in $[n]_2$, we conclude an important property as follows:

Theorem 5.1. *Given $n\in\mathbb{N}$, let m be an integer such that $[m]_2$ is obtained by either extending or truncating some runs of 0 or 1 of length $\geq k-1$ in $[n]_2$ to be different length but still $\geq k-1$. We have $b(CF_2(n!)) = b(CF_2(m!))$ and $u_q(CF_2(n!)) = u_q(CF_2(m!))$, and then*

$$CF_2(n!) \equiv_q CF_2(m!).$$

Proof. The proof of the second identity was stated in head of the theorem. The first one is due to the fact $b(CF_2(n!)) \equiv_2 zr(n)+n_1$ together with $zr(n)=zr(m)$ and $n_1=m_1$. The last equivalence is a direct consequence. ■

We use $\dot{n}$ to denote the integer such that $[\dot{n}]_2$ is obtained by truncating every run of 1 of length $\geq k$ in $[n]_2$ to be exactly length $k-1$, without changing any run of 0. Also let $\ddot{n}$ is the number obtained by truncating every run of 0 and run of 1 by the same way. For instance, let $k=3$ and $[n]_2=\langle 100011101111\rangle_2$ then $[\dot{n}]_2=\langle 100011011\rangle_2$ and $[\ddot{n}]_2=\langle 10011011\rangle_2$. Note that both $\dot{n}$ and $\ddot{n}$ depend on k, but we do not mark k for convenience. To avoid confusion, it should be remembered which k is discussed.

From (37), let us use the isomorphism $\mathbb{Z}_{16}^{*} \cong C_2 \times C_4$ in Table 1 to construct a new table as follows:

$s \in [3,13]_{\mathrm{o}} \subseteq \mathbb{Z}_{16}^{*}$	3	5	7	9	11	13
$u_{16}(s) \in C_4$	1	1	0	2	3	3
$\sum_{t\in[3,s]_{\mathrm{o}}} u_{16}(s) \pmod 4$	1	2	2	0	3	2

The last row of this table records the accumulations according to the second row. Now plug these accumulations into (38) and Lemma 5.1 to obtain

$$\begin{aligned} u_{16}(CF_2(n!)) &\equiv_4 \#(\mathcal{S}_4(\dot{n}),\{3,4\}) + 2\#(\mathcal{S}_4(\dot{n}),\{5,6,7,8,13,14\}) + 3\#(\mathcal{S}_4(\dot{n}),\{11,12\}) \\ &= \#(\mathcal{S}_4(\dot{n}),\{3,4,5^2,6^2,7^2,8^2,11^3,12^3,13^2,14^2\}) \end{aligned} \tag{39}$$

where the second line is a comprehensible modification for $\#(\cdot,\cdot)$ as weighted counting according each superscript. Notice that the weights of t (odd) and $t+1$ (even) are the same. Also notice that we can replace $\dot{n}$ with $\ddot{n}$ in this formula.

Since formula (39) is still too rough to use, we partition it into four disjoint parts and then simplify them. In the following, we consider $[t]_2$ and t the same element to plug into $\#(\mathcal{S}_4(\dot{n},\{\cdot\})$, and x means an unspecified binary digit.

$$\begin{aligned} A &:= \#(\mathcal{S}_4(\dot{n}),\{4\}) + 2\#(\mathcal{S}_4(\dot{n}),\{5,6,7\}) \\ &= \#(\mathcal{S}_4(\dot{n}),\{\langle 0100\rangle_2\}) + 2\big[\#(\mathcal{S}_4(\dot{n}),\{\langle 01\mathrm{xx}\rangle_2\}) - \#(\mathcal{S}_4(\dot{n}),\{\langle 0100\rangle_2\})\big] \\ &= 2r(\lfloor \frac{\dot{n}}{4} \rfloor) - \#(\mathcal{S}_4(\dot{n}),\{\langle 0100\rangle_2\}) \\ &= 2[r(\dot{n}) - \dot{n}_1(1-\dot{n}_2) - \dot{n}_0(1-\dot{n}_1)] - \#(\mathcal{S}_4(\dot{n}),\{\langle 0100\rangle_2\}); \end{aligned}$$

$$\begin{aligned} B &:= 3\#(\mathcal{S}_4(\dot{n})\{12\}) + 2\#(\mathcal{S}_4(\dot{n}),\{13,14\}), \\ &= 3\#(\mathcal{S}_4(\dot{n})\{\langle 1100\rangle_2\}) + 2\big[\#(\mathcal{S}_4(\dot{n}),\{\langle 11\mathrm{xx}\rangle_2\}) - \#(\mathcal{S}_4(\dot{n}),\{\langle 1100\rangle_2\})\big] \qquad (40) \\ &= 2\#(\mathcal{S}_4(\dot{n}),\{\langle 11\mathrm{xx}\rangle_2\}) + \#(\mathcal{S}_4(\dot{n})\{\langle 1100\rangle_2\}) \\ &= 2c_2(\lfloor \frac{\dot{n}}{4} \rfloor) + \#(\mathcal{S}_4(\dot{n}),\{\langle 1100\rangle_2\}) \\ &= 2[c_2(\dot{n}) - \dot{n}_0\dot{n}_1 - \dot{n}_1\dot{n}_2] + \#(\mathcal{S}_4(\dot{n}),\{\langle 1100\rangle_2\}); \\ C &:= \#(\mathcal{S}_4(\dot{n}),\{3\}) - \#(\mathcal{S}_4(\dot{n}),\{11\}) \\ &= \#(\mathcal{S}_4(\dot{n}),\{\langle 0011\rangle_2\}) - \big[\#(\mathcal{S}_4(\dot{n}),\{\langle \mathrm{x}011\rangle_2\}) - \#(\mathcal{S}_4(\dot{n}),\{\langle 0011\rangle_2\})\big] \\ &= 2\#(\mathcal{S}_4(\dot{n}),\{\langle 0011\rangle_2\}) - \#(\mathcal{S}_3(\dot{n}),\{\langle 011\rangle_2\}) \\ &= 2\#(\mathcal{S}_4(\dot{n}),\{\langle 0011\rangle_2\}) - r(\dot{n}) + r_1(\dot{n}); \qquad (41) \\ D &:= 2\#(\mathcal{S}_4(\dot{n}),\{8\}) \\ &= 2\#(\mathcal{S}_4(\dot{n}),\{\langle 1000\rangle_2\}) \end{aligned}$$

We obtain (40) because $\langle 11\mathrm{xx}\rangle_2$ has four types $[12]_2$, $[13]_2$, $[14]_2$, and $[15]_2 = \langle 1111\rangle_2$, but 15 never appears in $\mathcal{S}_4(\dot{n})$ for the truncation property of $\dot{n}$. We obtain (41) by referring to (25). Now collecting the four results above with a simple arrangement and referring to (26), we obtain

$$\begin{aligned}
u_{16}(CF_2(n!)) &\equiv_4 u_{16}(CF_2(\dot{n}!)) && (42)\\
&\equiv_4 2\big[r(\dot{n}) + c_2(\dot{n}) + \dot{n}_0 + \dot{n}_1 + \#(\mathcal{S}_4(\dot{n}), \{\langle 0011\rangle_2, \langle 1100\rangle_2, \langle 1000\rangle_2\})\big]\\
&\qquad + r_1(\dot{n}) - r(\dot{n}) - \#(\mathcal{S}_4(\dot{n}), \{\langle 0100\rangle_2, \langle 1100\rangle_2\})\\
&= 2\big[c_2(\dot{n}) + \dot{n}_0 + \dot{n}_1 + \#(\mathcal{S}_4(\dot{n}), \{\langle 0011\rangle_2, \langle 1\text{x}00\rangle_2\})\big]\\
&\qquad + r_1(\dot{n}) + r(\dot{n}) + zr_1(\dot{n}) - zr(\dot{n}). && (43)
\end{aligned}$$

Remark. In (40), we do use the property that $[\dot{n}]_2$ contains no sub-sequence $\langle 1^4\rangle_2$, whereas it does not matter for the existence of $\langle 0^4\rangle_2$ in $[\dot{n}]_2$. Therefore, to apply (43), truncating every run of 1 in $[n]_2$ is compulsory; however, truncating a run of 0 is optional. In other words, we can truncate or extend any run of 0 as long as we maintain the length $\geq k-1$.

We are ready to develop $u_{16}(CF_2(c_n))$. For this problem, we interpret $[n]_2$ as its two segments $[2\alpha]_2$ and $\langle 1^\beta\rangle_2$ defined in (30). Similarly, $[\dot{n}]_2$ also has its own two principal segments, which shall be $[2\dot{\alpha}]_2$ and $\langle 1^{\beta'}\rangle_2$ with $\beta' = \min\{\beta, 3\}$. We have

$$u_{16}(CF_2(n+1)) = u_{16}(2\alpha+1) = u_{16}(2\dot{\alpha}+1) = u_{16}(CF_2(\dot{n}+1)),$$

where the two u_{16}'s are equal because they depend respectively on the identical 3-segments $\langle \alpha_2\alpha_1\alpha_0\rangle_2$ and $\langle \dot{\alpha}_2\dot{\alpha}_1\dot{\alpha}_0\rangle_2$ (see (16)). This is why we use $\dot{n}$ instead of $\ddot{n}$. Actually, the only situation we are concerned about is that $\alpha \neq 0$ and $\langle \alpha_2\alpha_1\alpha_0\rangle_2 = \langle 000\rangle_2$. For instance, let $[n]_2 = \langle 100001\rangle_2$, and so $[\dot{n}]_2 = \langle 100001\rangle_2$ and $[\ddot{n}]_2 = \langle 10001\rangle_2$. We have $u_{16}(CF(n+1)) = u_{16}(CF(\dot{n}+1)) = 0$ but $u_{16}(CF(\ddot{n}+1)) = 2$. Using $\ddot{n}$ will cause an error in enumerating $u_{16}(CF_2(c_n))$.

Following the idea in the last paragraph, we will claim another important and useful theorem. Given $n \in \mathbb{N}$, let $\bar{n}$ be the integer such that $[\bar{n}]_2$ is obtained by the following rules.

a. When the rightmost run of 0 in $[n]_2$ is of length $\geq k+1$, let us truncate it to be length k, otherwise keep it the same.

b. For any other run of 0 or 1 of $[n]_2$ with length $\geq k$, truncate them to be length $k-1$.

Suppose $[n]_2$ is interpreted as its two principal segments $[2\alpha]_2$ and $\langle 1^\beta\rangle_2$ defined in (30). Interestingly, the corresponding two segments of $[\bar{n}]_2$ are exactly $[2\ddot{\alpha}]$ and $\langle 1^{\beta'}\rangle_2$, where $\beta' = \min\{\beta, k-1\}$. Moreover, we have

$$u_q(CF_2((2n)!)) \equiv_{q/4} u_q(CF_2(\bar{2n}!)) \equiv_{q/4} u_q(CF_2((2\bar{n})!)). \tag{44}$$

The second equivalence is a little bit complicated and takes time to understand. It is better to refer to the last remark.

Theorem 5.2. *Let $n, k \in \mathbb{N}$ with $k \geq 3$ and $\alpha = (CF_2(n+1)-1)/2$. We have*

$$c_n \equiv_{2^k} \begin{cases} c_{\bar{n}} & \text{for } d(\alpha) \leq k-1, \text{ and} \\ 0 & \text{for } d(\alpha) \geq k. \end{cases}$$

Proof. By Theorem 4.4, $c_n \equiv_{2^k} (-1)^{zr(\alpha)} 2^{d(\alpha)} 5^{u_q(CF_2(c_n))}$; so the condition for $c_n \equiv_{2^k} 0$ is trivial. Considering $d(\alpha) \leq k-1$ and using the fact that $c_{\bar{n}} \equiv_{2^k} (-1)^{zr(\ddot{\alpha})} 2^{d(\ddot{\alpha})} 5^{u_q(CF_2(c_{\bar{n}}))}$. we obtain that $d(\alpha) = d(\ddot{\alpha})$ and $zr(\alpha) = zr(\ddot{\alpha})$. The proof immediately follows, after we derive

$$\begin{aligned} u_q(CF_2(c_n)) &= u_q(CF_2((2n)!)) - u_q(CF_2(n+1)) - 2\,u_q(CF_2(n!)) \\ &\equiv_{q/4} u_q(CF_2((2\bar{n})!)) - u_q(CF_2(2\alpha+1)) - 2\,u_q(CF_2(\bar{n}!)) \\ &\equiv_{q/4} u_q(CF_2((2\bar{n})!)) - u_q(CF_2(2\ddot{\alpha}+1)) - 2\,u_q(CF_2(\bar{n}!)) \\ &= u_q(CF_2(c_{\bar{n}})). \end{aligned}$$

∎

Remark. The reason for the rightmost run of 0 banned on truncating into length $k-1$ is due to the enumeration of $u_q(CF_2(n+1))$.

Does every number in $[0, 2^k-1]$ admit to be a congruence of $c_n \pmod{2^k}$? Theorem 5.2 supports a negative answer as follows.

Theorem 5.3. *Let $k \geq 2$ and $q = 2^k$. (a) If there exists $\delta \in [0, k-1]$ such that $k^{\delta+1} < 2^{k-\delta-1}$, then there exists $N \in [0, q-1]$ with $\omega(N) = \delta$ such that $c_n \not\equiv_q N$ for any n. (b) The set of congruence numbers c_n (mod q) is a proper subset of $[0, q-1]$, and the cardinality of this set is bounded by $1 + \sum_{\delta=0}^{k-1} \min(k^{\delta+1}, 2^{k-\delta-1})$.*

Proof. To prove part (a), we need to find a upper bound for the cardinality of $\{[\bar{n}]_2 \mid n \in \mathbb{N} \text{ with } \omega_2(c_n) = \delta\}$. As usual, we split $[n]_2$ into two principal segments, $[2\alpha]_2$ and $\langle 1^\beta \rangle_2$. We are provided by $d(\alpha) = \omega_2(c_n) = \delta \leq k-1$. In the same way, $[\bar{n}]_2$ has its own principal segments, which must be $[2\ddot{\alpha}]$ and $\langle 1^{\beta'} \rangle_2$ with $d(\ddot{\alpha}) = \delta$ and $\beta' = \min\{\beta, k-1\}$. The last two identities suggest the possible types of $[\bar{n}]_2$. There are k^δ possible $\ddot{\alpha}$, and k possible β'; so we have $k^{\delta+1}$ possible $\bar{n}$. On the other hand, there are at most $2^{k-\delta-1}$ possible congruences to match these c_n (mod q). Therefore, the first assertion follows.

Now we prove part (b). As $k = 2$, we already know $c_n \not\equiv_4 3$. For $k \geq 3$, jut let $\delta = 0$ and then $k^{\delta+1} = k < 2^{k-1}$ is always true. The bound for the cardinality is a direct result from part (a). ∎

This property appeared in Theorem 4.7 as $(k, \delta) = (3, 0)$. It will appear again in Theorem 5.5 as $(k, \delta) = (4, 0)$ and in Theorem 6.6 as $(k, \delta) = (6, 0)$. However, in Theorem 6.4 we have $k^{\delta+1} > 2^{k-\delta-1}$ provided by $(k, \delta) = (6, 1)$, but some congruence numbers are still missing.

Using (44) and also plugging $\bar{n}$ into (43) instead of $\dot{n}$, we derive that

$$\begin{aligned} u_{16}(CF_2(c_n)) &\equiv_4 u_{16}(CF_2((2\bar{n})!)) - 2u_{16}(CF_2(\bar{n}!)) - u_{16}(CF_2(\bar{n}+1)) \qquad (45) \\ &\equiv_4 2\big[c_2(\bar{n}) + \bar{n}_0 + \bar{n}_2 + \bar{n}_0\bar{n}_2 + \#(\mathcal{S}_4(\bar{n}), \{\langle 0011\rangle_2, \langle 1\mathrm{x}00\rangle_2\})\big] \\ &\quad -r_1(\bar{n}) - r(\bar{n}) - zr_1(\bar{n}) + zr(\bar{n}) - \bar{n}_1 + \bar{n}_0\bar{n}_1 - u_{16}(CF_2(2\ddot{\alpha}+1)) \\ &\equiv_4 2\big[c_2(\bar{n}) + (1-\bar{n}_0)(1-\bar{n}_2) + \#(\mathcal{S}_4(\bar{n}), \{\langle 0011\rangle_2, \langle 1\mathrm{x}00\rangle_2\})\big] \\ &\quad +1 - r_1(\bar{n}) - zr_1(\bar{n}) + (1-\bar{n}_0)(1-\bar{n}_1) - [\ddot{\alpha}_0 + \ddot{\alpha}_1 + 2\ddot{\alpha}_2 - 2\ddot{\alpha}_0\ddot{\alpha}_1] \qquad (46) \\ &\equiv_4 \chi(\beta'=0)(2\ddot{\alpha}_1 - \ddot{\alpha}_0 - 1) - \chi(\beta'=1) + 2\chi(\beta'=2)\ddot{\alpha}_0 + 2\chi(\beta'=3)(1-\ddot{\alpha}_0) \\ &\quad +2\big[c_2(\ddot{\alpha}) + \ddot{\alpha}_0(1-\ddot{\alpha}_2) + \#(\mathcal{S}_4(\ddot{\alpha}), \{\langle 0011\rangle_2, \langle 1\mathrm{x}00\rangle_2\})\big] - r_1(\ddot{\alpha}) \\ &\quad -zr_1(\ddot{\alpha}) + \ddot{\alpha}_0\ddot{\alpha}_1 + 1. \qquad (47) \end{aligned}$$

To derive (46), we need the identity $r(\bar{n}) - zr(\bar{n}) = \bar{n}_0$ and refer to (16). With the help of (47), we can turn $d(\alpha) = k - 3$ to be a solved case for the problem of $c_n \pmod q$.

Corollary 5.4. *Let $n, k \in \mathbb{N}$, $\alpha = (CF_2(n+1) - 1)/2$ and $k - d(\alpha) = 3$. Then we have*

$$c_n \equiv_q (-1)^{zr(\alpha)} \big[2^{k-3} + 2^{k-1} u_{16}(CF_2(c_n))\big]. \tag{48}$$

Proof. Let us apply Theorem 4.4 and derive that

$$\begin{aligned} c_n &\equiv_q (-1)^{zr(\alpha)} 2^{d(\alpha)} (1+4)^{u_q(CF_2(c_n))} \\ &\equiv_q (-1)^{zr(\alpha)} 2^{k-3} \big[1 + 4\, u_q(CF_2(c_n))\big] \\ &\equiv_q (-1)^{zr(\alpha)} 2^{k-3} \big[1 + 4\, u_{16}(CF_2(c_n))\big], \end{aligned}$$

where the last equivalence is due to $u_q(t) \equiv_2 u_{16}(t)$, a result of Lemma 3.1. ■

Finally, we state and prove our main result of this section.

Theorem 5.5. *Let c_n be the n-th Catalan number. First of all, $c_n \not\equiv_{16} 3, 7, 9, 11, 15$ for any n. As for the other congruences, we have*

$$c_n \equiv_{16} \begin{cases} \left.\begin{array}{r} 1 \\ 5 \\ 13 \end{array}\right\} & \text{if} \quad d(\alpha) = 0 \text{ and } \quad \begin{cases} \beta \le 1, \\ \beta = 2, \\ \beta \ge 3, \end{cases} \\ \left.\begin{array}{r} 2 \\ 10 \end{array}\right\} & \text{if} \quad d(\alpha) = 1,\ \alpha = 1 \text{ and } \begin{cases} \beta = 0 \text{ or } \beta \ge 2, \\ \beta = 1, \end{cases} \\ \left.\begin{array}{r} 6 \\ 14 \end{array}\right\} & \text{if} \quad d(\alpha) = 1,\ \alpha \ge 2 \text{ and } \begin{cases} (\alpha = 2, \beta \ge 2) \text{ or } (\alpha \ge 3, \beta \le 1), \\ (\alpha = 2, \beta \le 1) \text{ or } (\alpha \ge 3, \beta \ge 2), \end{cases} \\ \left.\begin{array}{r} 4 \\ 12 \end{array}\right\} & \text{if} \quad d(\alpha) = 2 \text{ and } \quad \begin{cases} zr(\alpha) \equiv_2 0, \\ zr(\alpha) = 1, \end{cases} \\ \quad 8 & \text{if} \quad d(\alpha) = 3, \\ \quad 0 & \text{if} \quad d(\alpha) \ge 4. \end{cases}$$

where $\alpha = (CF_2(n+1) - 1)/2$ and $\beta = \omega_2(n+1)$ (or $\beta = \min\{i \mid n_i = 0\}$).

Proof. Congruences $0, 4, 8$ and 12 are trivial cases. Suppose $d(\alpha) = 1$ (so $\alpha \ge 1$). Here $b(CF_2(c_n)) = zr(\alpha)$ can only be 0 or 1 depending on $\alpha = 1$ or $\alpha \ge 2$ respectively. Moreover, $u_8(CF_2(c_n)) \equiv_2 \chi(\alpha = 2) + \chi(\beta = 1) + \chi(\alpha \ge 2)\chi(\beta \ge 1)$ by (35). Let us use the following table of $(b(CF_2(c_n)), u_8(CF_2(c_n)))$ for discussion.

	$\alpha = 1$	$\alpha = 2$	$\alpha \ge 3$
$\beta = 0$	(0,0)	(1,1)	(1,0)
$\beta = 1$	(0,1)	(1,1)	(1,0)
$\beta \ge 2$	(0,0)	(1,0)	(1,1)

We conclude the congruences $2, 6, 10, 14$ by using this table and referring to the isomorphism $Z_8^* \cong C_2 \times C_2$ in Table 1. For instance, if $(\alpha, \beta) = (2, 1)$ then $(b(CF_2(c_n)), u_8(CF_2(c_n))) = (1, 1)$. Hence $CF_2(c_n) \equiv_8 7$ and then $c_n \equiv_{16} 2 \times 7 = 14$. For $d(\alpha) = k - 3$, we can also use Lemma 5.4 to obtain the same result.

Now suppose $d(\alpha) = 0$. Clearly, $\alpha = 0$ and $b(CF_2(c_n)) = zr(\alpha) = 0$. Let us adopt a new notation $\bar{n}$ such that $[2\ddot{\alpha}]_2$ and $\langle 1^{\beta'}\rangle_2$ are the principal segments of $[\bar{n}]_2$. Notice that $\beta' = \min\{\beta, 3\}$. Since $\ddot{\alpha} = 0$ (due to $\alpha = 0$), every term involving $\ddot{\alpha}$ in (47) turns to 0. Thus, we have $u_{16}(CF_2(c_n)) = -\chi(\beta' = 0) - \chi(\beta' = 1) + 2\chi(\beta' = 3) + 1$, which equals $0, 0, 1, 3$ if $\beta' = 0, 1, 2, 3$ respectively. The congruences $1, 5, 13$ are done by case-discussion and referring to Table 1. ■

The lack of congruences $3, 7, 11, 15$ with respect to modulus 16 is inherited from the lack of $3, 7$ with respect to modulus 8 in Theorem 4.1, but the lack of 9 is a new result.

6 $u_{32}(CF_2(n!))$ and $u_{64}(CF_2(n!))$; $c_n \pmod{64}$

First, let us show the easy cases without proof: $c_n \equiv_{64} 0, 16.32$ or 48, as provided by $d(\alpha) \geq 4$.

Theorem 6.1. *Given $n \in \mathbb{N}$ with $\alpha = (CF_2(n+1) - 1)/2$, we have*

$$c_n \equiv_{64} \begin{cases} \left.\begin{matrix} 16 \\ 48 \end{matrix}\right\} & \text{if} \quad d(\alpha) = 4 \ \text{and} \quad \left\{\begin{matrix} zr(\alpha) \equiv_2 0 \\ zr(\alpha) \equiv_2 1, \end{matrix}\right. \\ 32 & \text{if} \quad d(\alpha) = 5, \\ 0 & \text{if} \quad d(\alpha) \geq 6. \end{cases}$$

The next class is for $c_n \equiv_{64} 8, 24, 40$ or 56.

Theorem 6.2. *Given $n \in \mathbb{N}$ with $d(\alpha) = 3$, we suppose $[\alpha]_2 = \langle 10^a 10^b 10^c\rangle_2$, i.e., $[n]_2 = \langle 10^a 10^b 10^{c+1} 1^\beta\rangle_2$. Also we define*

$$\begin{aligned} B &:= \chi(a \geq 1) + \chi(b \geq 1) + \chi(c \geq 1) \ \text{and} \\ U &:= \chi(a = 1) + \chi(b = 1) + \chi(c = 1) + \chi(b \geq 1)[\chi(a \geq 1) + \chi(c = 0)] + \chi(\beta \geq 2) + 1. \end{aligned}$$

Then we have

$$c_n \equiv_{64} \begin{cases} 8 & \text{if} \quad B \equiv_2 0 \quad \text{and} \quad U \equiv_2 0, \\ 24 & \text{if} \quad B \equiv_2 1 \quad \text{and} \quad U \equiv_2 0, \\ 40 & \text{if} \quad B \equiv_2 0 \quad \text{and} \quad U \equiv_2 1, \\ 56 & \text{if} \quad B \equiv_2 1 \quad \text{and} \quad U \equiv_2 1. \end{cases}$$

or simply

$$c_n \equiv_{64} 8 \times [4\chi(U \equiv_2 1) + 2\chi(B \equiv_2 1) + 1].$$

Proof. Because $d(\alpha) = 3$ we have $\omega_2(c_n) = 3$ and $CF_2(c_n) = 1, 3, 5, 7$. To determine the value of $CF_2(c_n)$ we shall refer to $T_8(CF_2(c_n))$. Now use (31) and (35) to interpret $T_8(CF_2(c_n))$ as follows:

$$b(CF_2(c_n)) \equiv_2 zr(\alpha) = \chi(a \geq 1) + \chi(b \geq 1) + \chi(c \geq 1),$$

which is B, and

$$\begin{aligned} u_8(CF_2(c_n)) &\equiv_2 \chi(\beta \geq 2) + \chi(\alpha = 1, \beta = 0) + r(\alpha) + r_1(\alpha) + zr_1(\alpha) + \alpha_0(1 - \alpha_1) \\ &= \chi(\beta \geq 2) + 0 + [1 + \chi(a \geq 1) + \chi(b \geq 1)] + [\chi(a \geq 1) + \chi(b \geq 1) \\ &\quad + \chi(a \geq 1)\chi(b \geq 1)] + [\chi(a = 1) + \chi(b = 1) + \chi(c = 1)] \\ &\quad + \chi(b \geq 1, c = 0), \end{aligned}$$

which is U after simplifying. ■

For those $c_n \pmod{64}$ with $\omega_2(c_n) = 2$, we can simply plug $u_{16}(c_n)$ given in (47) into (32). Here we also show a precise classification by tables.

Theorem 6.3. *Let $n \in \mathbb{N}$ with $d(\alpha) = 2$. Then we have*

$$c_n \equiv_{64} (-1)^{zr(\alpha)} 4 \times 5^{u_{16}(CF_2(c_n))},$$

where $u_{16}(CF_2(c_n))$ is given in (47). Precisely, let $[\alpha]_2 = \langle 10^a 10^b \rangle_2$, i.e., $[n]_2 = \langle 10^a 10^{b+1} 1^\beta \rangle_2$, and then we have c_n (mod 64) shown in the following four tables.

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	4	28	44	12
$b=1$	12	36	52	20
$b=2$	60	20	36	4
$b\geq 3$	28	52	4	36

when $\beta = 0$

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	52	12	28	60
$b=1$	44	4	20	52
$b=2$	60	20	36	4
$b\geq 3$	28	52	4	36

when $\beta = 1$

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	36	28	44	12
$b=1$	28	20	36	4
$b=2$	44	36	52	20
$b\geq 3$	12	4	20	52

when $\beta = 2$

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	4	60	12	44
$b=1$	60	52	4	36
$b=2$	12	4	20	52
$b\geq 3$	44	36	52	20

when $\beta \geq 3$

Proof. Notice that there are difference between $a \geq 3$ and $a = 3$, and similarly for b and β. We split (47) into two parts as follows:

$$\begin{aligned}
A &:= \chi(\beta'=0)(2\ddot{\alpha}_1 - \ddot{\alpha}_0 - 1) - \chi(\beta'=1) + 2\chi(\beta'=2)\ddot{\alpha}_0 + 2\chi(\beta'=3)(1-\ddot{\alpha}_0),\\
B &:= 2\big[c_2(\ddot{\alpha}) + \ddot{\alpha}_0(1-\ddot{\alpha}_2) + \#(\mathcal{S}_4(\ddot{\alpha}), \{\langle 0011\rangle_2, \langle 1\mathrm{x}00\rangle_2\})\big] - r_1(\ddot{\alpha}) - zr_1(\ddot{\alpha})\\
&\quad\; + \ddot{\alpha}_0\ddot{\alpha}_1 + 1.
\end{aligned}$$

Clearly, B is independent on β'. We will only prove the first table of this theorem. The other three tables can be checked in the same way. With simple calculation we obtain the values of A as $\beta = 0$ and B as follows:

	$a=0$	$a=1$	$a=2$	$a=3$
$b=0$	0	2	2	2
$b=1$	1	1	1	1
$b=2$	3	3	3	3
$b=3$	3	3	3	3

value of A when $\beta = 0$

	$a=0$	$a=1$	$a=2$	$a=3$
$b=0$	0	2	1	3
$b=1$	0	1	2	0
$b=2$	3	2	3	1
$b=3$	1	0	1	3

value of B

These two tables contribute u. Since we also know $b(CF_2(c_n)) \equiv_2 zr(\alpha) = \chi(a \geq 1) + \chi(b \geq 1)$, we obtain (b, u) as follows:

	$a=0$	$a=1$	$a=2$	$a=3$
$b=0$	$(0,0)$	$(1,0)$	$(1,3)$	$(1,1)$
$b=1$	$(1,1)$	$(0,2)$	$(0,3)$	$(0,1)$
$b=2$	$(1,2)$	$(0,1)$	$(0,2)$	$(0,0)$
$b=3$	$(1,0)$	$(0,3)$	$(0,0)$	$(0,2)$

Now refer to the isomorphism $\mathbb{Z}_{16}^* \cong C_2 \times C_4$ in Table 1 to obtain the corresponding numbers, and then multiply each of them by 4 to justify the first table of this theorem. ∎

Remark. No congruence is missing in the previous two theorems. But, in the remaining two classes in the following, some congruences will never been achieved, just like $c_4 \not\equiv_4 3$.

To settle down the remaining congruences of $c_n \pmod{64}$, we need to further deal with $u_{32}(CF_2(n!))$ and $u_{64}(CF_2(n!))$. Let us mimic the last section by using the isomorphism $\mathbb{Z}_{32}^* \cong C_2 \times C_8$ in Table 1 as follows:

$t \in \mathbb{Z}_{32}^*$	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
$u_{32}(t) \in C_8$	7	1	6	6	1	7	0	4	3	5	2	2	5	3	4
$\sum_{s\in[3,t]_o} u_{32}(s) \pmod 8$	7	0	6	4	5	4	4	0	3	0	2	4	1	4	0

So we have

$$\begin{aligned} u_{32}(CF_2(n!)) \;&\equiv_8\; \#(\mathcal{S}_5(\ddot{n}), \{3^7, 4^7, 7^6, 8^6, 9^4, 10^4, 11^5, 12^5, 13^4, 14^4, 15^4, 16^4, 19^3, 20^3, \\ &\qquad 23^2, 24^2, 25^4, 26^4, 27, 28, 29^4, 30^4\}) \\ &=: \;\phi_{32}(\mathcal{S}_5(\ddot{n})). \end{aligned} \tag{49}$$

In this formula, $\ddot{n}$ can be replaced by n, $\dot{n}$ or $\bar{n}$. Unlike our operation from (39) to (43), we are not going to simplify this formula, because it is good enough to deal with $c_n \pmod{64}$; nevertheless, it would be worth developing a simpler form in the future. Above, we also define $\phi_{32}(\mathcal{S}_5(\ddot{n}))$ to be the right hand side of (49), in order to plug into ϕ_{32} with some other multi-sets instead of $\mathcal{S}_5(\ddot{n})$. In the following, we set $\phi_{32}(\{[t]_2\}) := \phi_{32}(\{t\})$ for convenience.

$$\begin{aligned} u_{32}(CF_2(c_n)) \;&\equiv_8\; \phi_{32}(\mathcal{S}_5(2\ddot{n})) - 2\phi_{32}(\mathcal{S}_5(\ddot{n})) - u_{32}(CF_2(\bar{n}+1)) \\ &\equiv_8\; \phi_{32}(\{\langle \ddot{n}_3\ddot{n}_2\ddot{n}_1\ddot{n}_0 0\rangle_2\}) - \phi_{32}(\mathcal{S}_5(\ddot{n})) - u_{32}(\langle \ddot{\alpha}_3\ddot{\alpha}_2\ddot{\alpha}_1\ddot{\alpha}_0 1\rangle_2). \end{aligned} \tag{50}$$

By this formula, we can classify $c_n \pmod{64}$ for those n with $d(\alpha) = 1$ as follows:

Theorem 6.4. *Let $n \in \mathbb{N}$ with $d(\alpha) = 1$. The congruences of c_n (mod 64) are classified by the following table.*

	$\alpha=1$	$\alpha=2$	$\alpha=2^2$	$\alpha=2^3$	$\alpha=2^s$
$\beta=0$	2	14	22	38	6
$\beta=1$	42	62	54	38	6
$\beta=2$	34	22	14	62	30
$\beta=3$	18	6	62	46	14
$\beta\geq 4$	50	38	30	14	46

where $s \geq 4$.

Proof. Adopt $[\ddot{\alpha}]_2$ and $\langle 1^{\beta'}\rangle_2$ as the two principal segments of $[\bar{n}]_2$ for $k=5$ (not 6). We shall have $d(\ddot{\alpha})=d(\alpha)=1$ and $\beta'=\min\{\beta,5\}$. We use (31) and (50) to obtain the next table for $(b(CF_2(c_n)), u_{32}(CF_2(c_n)))$ as follows:

	$\ddot{\alpha}=1$	$\ddot{\alpha}=2$	$\ddot{\alpha}=2^2$	$\ddot{\alpha}=2^3$	$\ddot{\alpha}=2^4$
$\beta'=0$	$(0,0)$	$(1,6)$	$(1,1)$	$(1,3)$	$(1,7)$
$\beta'=1$	$(0,5)$	$(1,4)$	$(1,5)$	$(1,3)$	$(1,7)$
$\beta'=2$	$(0,4)$	$(1,1)$	$(1,6)$	$(1,4)$	$(1,0)$
$\beta'=3$	$(0,6)$	$(1,7)$	$(1,4)$	$(1,2)$	$(1,6)$
$\beta'=4$	$(0,2)$	$(1,3)$	$(1,0)$	$(1,6)$	$(1,2)$

Now find every corresponding number by referring to the isomorphism $\mathbb{Z}_{32}^*\cong C_2\times C_{16}$ in Table 1, and then multiply the number by 2 to obtain the table in this theorem. ■

Corollary 6.5. *We have* $c_n\not\equiv_{64} 10, 26$ *and* 58.

The final class will be solved after we realize $u_{64}(CF_2(c_n))$. Here we skip some detail, especially a huge table for the sum $\sum_{t\in[3,s]_o} u_{64}(s)$ (mod 16). We show the formulae of $u_{64}(CF_2(n!))$ and $u_{64}(CF_2(c_n))$ directly as follows:

$$\begin{aligned} u_{64}(CF_2(n!)) &\equiv_{16} \#(\mathcal{S}_6(\ddot{n}), \{3^{11},4^{11},5^{12},6^{12},7^{14},8^{14},9^4,10^4,11,12,15^{12},16^{12},17^8,18^8,\\ &\qquad 19^7,20^7,21^4,22^4,23^{10},24^{10},25^{12},26^{12},27^{13},28^{13}29^8,30^8,31^8,32^8,\\ &\qquad 35^3,36^3,37^{12},38^{12},39^6,40^6,41^4,42^4,43^9,44^9,47^4,48^4,49^8,50^8,\\ &\qquad 51^{15},52^{15},53^4,54^4,55^2,56^2,57^{12},58^{12},59^5,60^5,61^8,62^8\}) \qquad (51)\\ &=: \phi_{64}(\mathcal{S}_6(\ddot{n}));\\ u_{64}(CF_2(c_n)) &\equiv_{16} \phi_{64}(\mathcal{S}_6(2\ddot{n}))-2\phi_{64}(\mathcal{S}_6(\ddot{n}))-u_{64}(CF_2(\bar{n}+1))\\ &\equiv_{16} \phi_{64}(\{\langle \ddot{n}_4\ddot{n}_3\ddot{n}_2\ddot{n}_1\ddot{n}_0 0\rangle_2\})-\phi_{64}(\mathcal{S}_6(\ddot{n}))-u_{64}(\langle\ddot{\alpha}_4\ddot{\alpha}_3\ddot{\alpha}_2\ddot{\alpha}_1\ddot{\alpha}_0 1\rangle_2). \qquad (52) \end{aligned}$$

The following theorem is directly checked by (52); so we skip its proof. On the other hand, by Theorem 5.2, we can verify this theorem by only enumerating $c_0, c_1, c_3, c_7, c_{15}$, and c_{31} (mod 64).

Theorem 6.6. *Let* $n\in\mathbb{N}$ *with* $d(\alpha)=0$*, i.e.* $n=2^\beta-1$*. Then we have*

$$c_n \equiv_{64} \begin{cases} 1 & \text{if } \beta=0 \text{ or } 1;\\ 5 & \text{if } \beta=2;\\ 45 & \text{if } \beta=3;\\ 61 & \text{if } \beta=4;\\ 29 & \text{if } \beta\geq 5.\end{cases}$$

Moreover, any number in $[0,63]_o-\{1,5,29,45,61\}$ *can never be the congruence of* c_n *(mod 64).*

7 Future research and acknowledgements

The odd congruences of $c_n \pmod{2^k}$ happen if and only if $n = 2^m - 1$ for $m \in \mathbb{N}$. After observing all odd congruences from modulus 4 up to modulus 1024, once we conjectured the following property. It was soon proved by H.-Y. Lin [15].

Theorem 7.1. *Let $k \geq 2$. There only exist $k-1$ different odd congruences $c_n \pmod{2^k}$, and they are $c_{2^m-1} \pmod{2^k}$ for $m = 1, 2, \ldots, k-1$.*

In other words, if $n = 2^m - 1$ then $c_n \pmod{2^k}$ are distinct odd integers for $m = 1, 2, \ldots, k-1$. Associated with this theorem, there are a trivial fact $c_0 \equiv_{2^k} c_1 \equiv_{2^k} 1$ and a non-trivial fact $c_{2^m-1} \equiv_{2^k} c_{2^{k-1}-1}$ for each $m \geq k$ that directly follows Theorem 5.2.

The final interest is to develop a systematic algorithm for calculating the modularity of various combinatorial numbers. But that is a long-term goal. So far some further research directions in our mind are

(a) The congruences of $c_n \pmod{p^k}$ for some odd prime p, which is a continuation of the work of this paper;

(b) The congruences of some other combinatorial numbers modulo a prime power, in particular, $\binom{m}{n}$ and Motzkin numbers;

(c) A more efficient isomorphic machine exchanging between $\mathbb{Z}_{q^k}^*$ and the corresponding additive group, in order to facilitate the arguments of this paper;

(d) In case that part (c) is admissible for some higher power of a prime, we hope to derive an algorithm to enumerate congruences for various combinatorial numbers.

The second author thanks the Institute of Mathematics at the Academia Sinica for stimulating this joint work when she participated in the Summer School for Undergraduate Research held there. Both authors would like to thank Prof. Peter Shiue, Prof. Bruce Sagan and the anonymous referees for many comments and suggestions for improving the original version of this paper.

References

[1] R. Alter and K. K. Kubota, Prime and prime power divisibility of Catalan numbers, *J. Combin. Theory Ser. A* **15** (1973), 243–256.

[2] K. S. Davis and W. A. Webb, Lucas' theorem for prime powers, *European J. Combin.* **11** (1990), 229–233.

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

[4] E. Deutsch and B. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, *J. Number Theory* **117** (2006), 191–215.

[5] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, 1919 (Chapter XI).

[6] R. Donaghey and L. W. Shapiro, Motzkin Numbers, *J. Combin. Theory Ser. A* **23** (1977), 291–301.

[7] S.-P. Eu, S.-C. Liu, and Y.-N. Yeh, On the congruences of some combinatorial numbers, *Stud. Appl. Math.* **116** (2006), 135–144.

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

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

[10] I. M. Gessel, Some congruences for Apéry numbers, *J. Number Theory* **14** (1982), 362–368.

[11] A. Granville, Arithmetic properties of binomial coefficients I: binomial coefficients modulo prime powers, available at
http://www.cecm.sfu.ca/organics/papers/granville/index.html .

[12] A. Granville, Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's Triangle, *Amer. Math. Monthly* **99** (1992), 318–381.

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

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

[15] H.-Y. Lin, Odd Catalan numbers modulo 2^k, to appear in *European J. Combin.*

[16] F. Luca and M. Klazar, On integrality and periodicity of the Motzkin numbers, *Aequ. Math.* **69** (2005), 68–75.

[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] Y. Mimura, Congruence properties of Apery numbers, *J. Number Theory* **16** (1983), 138–146.

[19] A. Postnikov and B. Sagan, Note: What power of two divides a weighted Catalan number, *J. Combin. Theory Ser. A* **114** (2007), 970–977.

[20] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Springer, 1994.

[21] R. P. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge University Press, 1999.

[22] S. Wolfram, *A New Kind of Science*, Wolfram Media, 2002.

2010 *Mathematics Subject Classification*: Primary 05A10; Secondary 11B50.
Keywords: prime power modulus, Catalan numbers, Kummer's theorem, Lucas' theorem.

Received January 14 2010; revised version received April 30 2010. Published in *Journal of Integer Sequences*, May 3 2010.

Return to Journal of Integer Sequences home page.