Congruences of Finite Summations of the Coefficients in certain Generating Functions

Po-Yi Huang[*]

Department of Mathematics
National Cheng Kung University
Tainan City, Taiwan
pyhuang@mail.ncku.edu.tw

Shu-Chung Liu[†]

Department of Applied Mathematics
National Hsinchu University of Education
Hsinchu City, Taiwan
liularry@mail.nhcue.edu.tw

Yeong-Nan Yeh[‡]

Institute of Mathematics
Academia Sinica
Taipei, Taiwan
mayeh@math.sinica.edu.tw

Submitted: Sep 4, 2013; Accepted: May 25, 2014; Published: Jun 9, 2014
Mathematics Subject Classifications: 11B50, 05A15, 05A10

Abstract

In this paper we develop a general method to enumerate the congruences of finite summations $\sum_{k=0}^{p-1} \frac{a_k}{m^k} \pmod{p}$ and $\sum_{k=0}^{p-1-h} \frac{a_k a_{k+h}}{B^k} \pmod{p}$ for the infinite sequence $\{a_n\}_{n\geqslant 0}$ with generating functions $(1+xf(x))^{\frac{N}{2}}$, where $f(x)$ is an integer polynomial and N is an odd integer with $|N| < p$. We also enumerate the congruences of some similar finite summations involving generating functions $\frac{1-\alpha x-\sqrt{1-2(\alpha+\beta)x+Bx^2}}{\beta x}$ and $\frac{1-\alpha x-\sqrt{1-2\alpha x+(\alpha^2-4\beta)x^2}}{2\beta x^2}$.

1 Introduction

Let p be an odd prime number and m be an integer with $m \not\equiv 0 \pmod{p}$. The initial topic of this article is to enumerate

$$\sum_{k=0}^{p-1} \frac{a_k}{m^k} \pmod{p} \tag{1}$$

[*] Partially supported by NSC 100-2115-M-006-008.

[†] Corresponding author. Partially supported by NSC 101-2115-M-134-134-006.

[‡] Partially supported by NSC 101-2115-M-001-013-MY3.

the congruence of the pth partial sum of the infinite sequence $\{a_n\}_{n=0}^{\infty}$. The study of the congruence of a single term, $a_n \pmod p$, has a long history extending form the most famous and edge-old problem of Pascal's fractal, which is originally formed by the parities of binomial coefficients $\binom{n}{k}$ [5, 6, 13, 14, 15, 16, 19, 25], to the most recent works about Apéry numbers [2, 4, 9, 11, 20], central Delannoy numbers [9], Catalan numbers [1, 7, 10, 17, 21], Motzkin numbers [7, 9, 18] and etc. [12].

This article focuses on the sequence $\{a_n\}_{n=0}^{\infty}$ with generating functions (GF's) $(1 + xf(x))^{\frac{N}{2}}$, where $f(x)$ is an integer polynomial and N is an odd integer with $|N| < p$. Neither a_n nor $\frac{a_k}{m^k}$ in (1) is necessarily an integer if we deal with the field of rational numbers; therefore, we shall consider both a_n and $\frac{a_k}{m^k}$ the congruences in the modular arithmetic field with modulus p. For instance, usually $\binom{1/2}{k}$ is a fraction; however, in the modular arithmetic field $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, we have

$$\binom{\frac{1}{2}}{k} \equiv \binom{\frac{p+1}{2}}{k} \pmod p \quad \text{for } k = 0, 1, \ldots, p-1, \tag{2}$$

which is always an integer. For example let $p = 5$, and then $\binom{\frac{1}{2}}{2} = \left(\frac{1}{2} \cdot \frac{-1}{2}\right)/2! = \frac{-1}{8} \equiv 3 \pmod 5 = \binom{3}{2}$.

Z.-W. Sun [24] applied (2) and some other tools to verify the equivalence

$$\sum_{k=1}^{p-1} \frac{c_k}{m^k} \equiv \frac{m-4}{2}\left(1 - \left(\frac{m(m-4)}{p}\right)\right) \pmod p, \tag{3}$$

where c_k is the kth Catalan number and $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a; \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p; \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

One has the following well-known and useful congruence:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p, \text{ with } \left(\frac{a}{p}\right) \in \{-1, 0, 1\}. \tag{4}$$

In [24], Sun also derived $\sum_{k=1}^{p-1} \frac{a_k}{m^k} \pmod p$ for a_k being the kth central Delannoy number or Schröder number respectively. The results by Sun initiate the motivation of our study. In this article, we wish to provide a systematic method to deal with the problems of this kind.

The article is organized as follows. In Section 2, we exam the problem in (1) by generating functions. As applications, similar problems of (1) involving generating functions modified from $\sqrt{1 + Ax + Bx^2}$ are given in Section 3. In Section 4, we focus on another type of problem $\sum_{k=0}^{p-1-h} \frac{a_k a_{k+h}}{(\pm B)^k} \pmod p$. And then some applications are demonstrated in Sections 5 and 6.

2 GF's of the form $(1+xf(x))^{\frac{N}{2}}$

Let $\{a_k\}_{k\geqslant 0}$ be the sequence associating with the generating function

$$(1+xf(x))^{\frac{N}{2}},$$

where $f(x)$ is an integer polynomial and N is an odd integer with $|N|<p$. To formulate $\sum_{k=0}^{p-1} a_k m^k \pmod p$ and $\sum_{k=0}^{p-1} \frac{a_k}{m^k} \pmod p$, which are same problem in different forms, we need the following facts:

(i) $\binom{\frac{N}{2}}{k} \equiv \binom{\frac{p+N}{2}}{k} \pmod p$ for $k=0,1,\ldots,p-1$;

(ii) $\binom{\frac{N}{2}}{k} \equiv \binom{\frac{p+N}{2}}{k} \equiv 0 \pmod p$ for $k=\frac{p+N+2}{2},\ldots,p-1$;

(iii) $\binom{\frac{N}{2}}{p} \equiv -2^{-1} \pmod p$; moreover $\binom{\frac{N}{2}}{p+k} \equiv -2^{-1}\binom{\frac{p+N}{2}}{k} \pmod p$ for $k=0,1,\ldots,p-1$

The reason for (i) is trivial and the congruence 0 in (ii) is due to that $\frac{p+N}{2}$ is an integer and $k>\frac{p+N}{2}$. The reason for the first equivalence in (iii) is because of the bijection between $\{N, N-2,\cdots,N-2p+2\}$ and $\{0,1,\ldots p-1\}$ under modulo p; however, the element $N-2i$ such that $N-2i\equiv 0 \pmod p$ is $-p$, and additionally $2^{-p}\equiv 2^{-1} \pmod p$. The second equivalence in (iii) directly follows the first one. The advantage of (i) is that $\binom{\frac{p+N}{2}}{k}$ is a normal binomial coefficient; therefore, we can apply $\binom{\frac{p+N}{2}}{k} = \binom{\frac{p+N}{2}}{\frac{p+N}{2}-k}$.

In the following, the equivalence $f(x)\equiv g(x) \pmod{h(x)}$ means that $f(x)$ and $g(x)$ share same residue with respect to divisor $h(x)$. Moreover, $f(x)\equiv g(x) \pmod{x^q, p}$ indicates that the coefficients of $f(x)$ and $g(x)$ for the term x^k, with $k=0,1,\ldots,q-1$, are congruent modulo p.

Theorem 1. *Given an odd prime p and an integer m with $m\not\equiv 0 \pmod p$. Let $\{a_k\}_{k\geqslant 0}$ be a sequence of integers whose generating function is $(1+xf(x))^{\frac{N}{2}}$, where $f(x)$ is an integer polynomial and N is an odd integer with $|N|<p$. We have*

$$(1+xf(x))^{\frac{N}{2}} \equiv (1+xf(x))^{\frac{p+N}{2}} \pmod{x^p, p}, \quad \textit{and} \tag{5}$$

$$\sum_{k=0}^{p-1} a_k m^k \equiv (1+mf(m))^{\frac{N+1}{2}} \left(\frac{1+mf(m)}{p}\right) - E(m) \pmod p, \tag{6}$$

where $E(x)$ is the polynomial consisting of each terms x^t with $t\geqslant p$ in the expansion of $(1+xf(x))^{\frac{p+N}{2}}$.

Proof. Actually, (5) and (6) are equivalent. The following can prove both at the same time.

$$\sum_{k=0}^{p-1} a_k m^k = \left[(1+xf(x))^{\frac{N}{2}} \pmod{x^p}\right]_{x=m} \tag{7}$$

$$\begin{aligned}
&= \left[\sum_{k=0}^{p-1}\binom{\frac{N}{2}}{k}(xf(x))^k \pmod{x^p}\right]_{x=m} \\
&\equiv \left[\sum_{k=0}^{\frac{p+N}{2}}\binom{\frac{p+N}{2}}{k}(xf(x))^k \pmod{x^p, p}\right]_{x=m} && (8)\\
&= \left[(1+xf(x))^{\frac{p+N}{2}} - E(x)\right]_{x=m} && (9)\\
&\equiv (1+mf(m))^{\frac{N+1}{2}}\left(\frac{1+mf(m)}{p}\right) - E(m) \pmod{p}.
\end{aligned}$$

Notice that the equivalence in (8) responses to modulus p by applying (i) and (ii), and the equation in (9) yields by modulus x^p and that $\frac{p+N}{2}$ is an exponent of positive integer. The last equivalence is because of (4). Referring to (7) and (8) without substituting $x = m$, we then verify (5). □

It takes time to enumerate $E(x)$ unless $f(x)$ is simple enough. In the rest of this section we assume $f(x) = A + Bx$. Let $[x^n]g(x)$ denote the coefficient of x^n in the power series $g(x)$. We derive the following rules:

(r1) If $B \equiv 0 \pmod{p}$ then $E(x) \equiv 0 \pmod{p}$. Moreover, we have

$$\sum_{k=0}^{t} a_k m^k \equiv (1+mf(m))^{\frac{N+1}{2}}\left(\frac{1+mf(m)}{p}\right) \pmod{p},$$

for $t = \frac{p+N}{2}, \frac{p+N+2}{2}, \ldots, p-1$ due to $a_{\frac{p+N+2}{2}} \equiv \cdots \equiv a_{p-1} \equiv 0 \pmod{p}$ by (ii).

(r2) If $N \leqslant -1$ then $E(x) = 0$ again.

(r3) If $N \geqslant 1$ and $B \not\equiv 0 \pmod{p}$, then $E(x) \neq 0$. Let

$$(1 + Ax + Bx^2)^{\frac{p+N}{2}} = q_0 + q_1 x + \cdots + q_{p+N}x^{p+N}.$$

For the precise value of q_m, we can simply apply the following formula:

$$\begin{aligned}
&[x^e](1 + \alpha x + \beta x^2)^M \\
&\quad = \begin{cases} \sum_{k=\lceil \frac{e}{2}\rceil}^{\min\{e,M\}} \binom{M}{M-k,\,2k-e,\,e-k}\alpha^{2k-e}\beta^{e-k} & \text{if } M > 0 \text{ and } e \leqslant 2M; \\ \sum_{k=\lceil \frac{e}{2}\rceil}^{e} (-1)^k \binom{-M+k-1}{-M-1,\,2k-e,\,e-k}\alpha^{2k-e}\beta^{e-k} & \text{if } M < 0. \end{cases}
\end{aligned}$$

Therefore,

$$q_m = \sum_{k=\lceil \frac{m}{2}\rceil}^{\min\{m,\frac{p+N}{2}\}} \binom{\frac{p+N}{2}}{\frac{p+N}{2}-k,\,2k-m,\,m-k} A^{2k-m}B^{m-k}.$$

Particularly, if $N=1$ then $E(x) \equiv \frac{A}{2}\left(\frac{B}{p}\right) x^p + B\left(\frac{B}{p}\right) x^{p+1} \pmod p$; if $p>3$ and $N=3$ then

$$\begin{aligned} E(x) \;\equiv\; & \left(\frac{3}{2^2}A\left(\frac{B}{p}\right) - \frac{1}{2^4}A^3B^{-1}\left(\frac{B}{p}\right)\right)x^p + \left(\frac{3}{2}B\left(\frac{B}{p}\right) + \frac{3}{2^3}A^2\left(\frac{B}{p}\right)\right)x^{p+1} \\ & + \frac{3}{2}AB\left(\frac{B}{p}\right)x^{p+2} + B^2\left(\frac{B}{p}\right)x^{p+3} \pmod p. \end{aligned}$$

In case that $E(x)=0$, we reach a particular case as follows.

Corollary 2. *If $f(x)$ is a constant function or $f(x)=A+Bx$ with $N \leqslant -1$, then we have $E(x)=0$ and*

$$\sum_{k=0}^{p-1} \frac{a_k}{m^k} \equiv \left(\frac{m^2+Am+B}{m^2}\right)^{\frac{N+1}{2}} \left(\frac{m^2+Am+B}{p}\right) \pmod p.$$

Here we recall some sequences as applications of the last corollary:

sequence name	first few terms	GF	$\sum_{k=0}^{p-1}\frac{a_k}{m^k} \pmod p$
central binomial coeff.	$1,2,6,20,70,\dots$	$\frac{1}{\sqrt{1-4x}}$	$\left(\frac{m^2-4m}{p}\right)$
central trinomial coeff.	$1,1,3,7,19,51,\dots$	$\frac{1}{\sqrt{1-2x-3x^2}}$	$\left(\frac{m^2-2m-3}{p}\right)$
central Delannoy numbers	$1,3,13,63,321,\dots$	$\frac{1}{\sqrt{1-6x+x^2}}$	$\left(\frac{m^2-6m+1}{p}\right)$ (see [24])
A002457, in [22]	$1,6,30,140,630,\dots$	$(1-4x)^{\frac{-3}{2}}$	$\frac{m^2}{m^2-4m}\left(\frac{m^2-4m}{p}\right)$
A002420, in [22]	$1,-2,-2,-4,-10,\dots$	$\sqrt{1-4x}$	$\frac{m^2-4m}{m^2}\left(\frac{m^2-4m}{p}\right)$

Table 1: Some direct applications of Corollary 2

Let us take advance to enumerate $\sum_{k=0}^{p}\frac{a_k}{m^k}$ and $\sum_{k=0}^{p+1}\frac{a_k}{m^k}$, which will be used in the nest section. We need to enumerate two additional terms, $\frac{a_p}{m^p}$ and $\frac{a_{p+1}}{m^{p+1}}$. Using (4), (i), (ii) and (iii), we calculate a_p and a_{p+1} as follows:

$$\begin{aligned} [x^p](1+Ax+Bx^2))^{\frac{N}{2}} &= \sum_{k=0}^{p}[x^p]\binom{\frac{N}{2}}{k}(x(A+Bx))^k \\ &= \sum_{k=\frac{p+1}{2}}^{p}\binom{\frac{N}{2}}{k}[x^{p-k}](A+Bx)^k \\ &\equiv \binom{\frac{N}{2}}{\frac{p+1}{2}}[x^{\frac{p-1}{2}}](A+Bx)^{\frac{p+1}{2}} + \binom{\frac{N}{2}}{p}[x^0](A+Bx)^p \pmod p \end{aligned}$$

$$\begin{aligned}
&\equiv \binom{\frac{p+N}{2}}{\frac{p+1}{2}}\frac{p+1}{2}AB^{\frac{p-1}{2}}-\frac{1}{2}A^p \pmod p\\
&\equiv \frac{A}{2}\left(\binom{\frac{p+N}{2}}{\frac{p+1}{2}}\left(\frac{B}{p}\right)-1\right) \pmod p,
\end{aligned}$$

$$\begin{aligned}
[x^{p+1}](1+Ax+Bx^2))^{\frac{N}{2}} &= \sum_{k=\frac{p+1}{2}}^{p+1}\binom{\frac{N}{2}}{k}[x^{p-k+1}](A+Bx)^k\\
&\equiv \binom{\frac{N}{2}}{\frac{p+1}{2}}[x^{\frac{p+1}{2}}](A+Bx)^{\frac{p+1}{2}}+\binom{\frac{N}{2}}{p}[x](A+Bx)^p\\
&\qquad +\binom{\frac{N}{2}}{p+1}[x^0](A+Bx)^{p+1} \pmod p\\
&\equiv \binom{\frac{p+N}{2}}{\frac{p+1}{2}}B^{\frac{p+1}{2}}+0-\frac{1}{2}\binom{\frac{p+N}{2}}{1}A^{p+1} \pmod p\\
&\equiv \binom{\frac{p+N}{2}}{\frac{p+1}{2}}\left(\frac{B}{p}\right)B-\frac{N}{2^2}A^2 \pmod p.
\end{aligned}$$

If $B\equiv 0 \pmod p$ or $N\leqslant -1$, then $\sum_{k=0}^{p}\frac{a_k}{m^k}$ and $\sum_{k=0}^{p+1}\frac{a_k}{m^k}$ are ready because we have $\frac{a_p}{m^p}\equiv -\frac{A}{2m} \pmod p$, $\frac{a_{p+1}}{m^{p+1}}\equiv -\frac{NA^2}{4m^2} \pmod p$, $E(x)=0$ and referring (6). When $B\not\equiv 0 \pmod p$ and $N\geqslant 1$, then the larger N is, the more complicate $E(x)$ is. However the two summations for $N=1$ are also ready as follows.

Corollary 3. *Let $\{a_n\}_{n\geqslant 0}$ be the sequence whose generating function is $\sqrt{1+Ax+Bx^2}$. We have*

$$\begin{aligned}
\sum_{k=0}^{p}\frac{a_k}{m^k} &\equiv \frac{m^2+Am+B}{m^2}\left(\frac{m^2+Am+B}{p}\right)-\frac{A}{2m}-\frac{B}{m^2}\left(\frac{B}{p}\right) \pmod p,\\
\sum_{k=0}^{p+1}\frac{a_k}{m^k} &\equiv \frac{m^2+Am+B}{m^2}\left(\frac{m^2+Am+B}{p}\right)-\frac{A}{2m}-\frac{A^2}{4m^2} \pmod p.
\end{aligned}$$

3 GF's modified from $\sqrt{1+Ax+Bx^2}$

Many well-known sequences are associated with generating functions modified from $(1+Ax+Bx^2)^{\frac{1}{2}}$. In this section, we consider two types:

$$\frac{1-\alpha x-\sqrt{1-2(\alpha+\beta)x+Bx^2}}{\beta x} \quad\text{and}\quad \frac{1-\alpha x-\sqrt{1-2\alpha x+(\alpha^2-4\beta)x^2}}{2\beta x^2}.$$

Let $\frac{1-\alpha x-\sqrt{1-2(\alpha+\beta)x+Bx^2}}{\beta x}$ be the generating function of the sequence $\{b_n\}_{n\geqslant 0}$, and let $A=-2(\alpha+\beta)$ for convenience. For examples, $(\alpha,\beta,B)=(0,2,0)$ yields the Catalan number, $(1,2,1)$ and $(-1,4,1)$ provide the large and the little Schröder numbers respectively, and $(1,2,5)$ is associated with the number of restricted hexagonal polyominoes [22, A002212].

Theorem 4. *We have*

$$\sum_{k=0}^{p-1}\frac{b_k}{m^k} \equiv 1+\frac{m^2+Am+B}{\beta m}\left(1-\left(\frac{m^2+Am+B}{p}\right)\right)+\frac{B}{\beta m}\left(\left(\frac{B}{p}\right)-1\right) \pmod{p}.$$

Proof. We still let $\{a_n\}_{n\geqslant 0}$ associate with $\sqrt{1+Ax+Bx^2}$. Notice that $b_k=-\frac{a_{k+1}}{\beta}$ for $k\geqslant 1$. Also it is clear that $a_0=1$, $a_1=\frac{A}{2}$ and $b_0=1$.

$$\begin{aligned}\sum_{k=0}^{p-1}\frac{b_k}{m^k} &= 1-\frac{m}{\beta}\sum_{k=2}^{p}\frac{a_k}{m^k}\\ &= 1+\frac{m}{\beta}+\frac{A}{2\beta}-\frac{m}{\beta}\sum_{k=0}^{p}\frac{a_k}{m^k}\\ &\equiv 1+\frac{m}{\beta}+\frac{A}{2\beta}-\frac{m}{\beta}\left(\frac{m^2+Am+B}{m^2}\left(\frac{m^2+Am+B}{p}\right)-\frac{A}{2m}\right.\\ &\quad\left.-\frac{B}{m^2}\left(\frac{B}{p}\right)\right) \pmod{p},\\ &= 1+\frac{m^2+Am+B}{\beta m}\left(1-\left(\frac{m^2+Am+B}{p}\right)\right)+\frac{B}{\beta m}\left(\left(\frac{B}{p}\right)-1\right).\end{aligned}$$

□

In particular, the last term in the last theorem is zero if $B\equiv 0 \pmod{p}$ or $\left(\frac{B}{p}\right)=1$. This particular case happens for the Catalan numbers (see (3) and also [24, Lemma 2.1]), the large Schröder numbers (see [24, Theorem 1.2]) and the little Schröder numbers.

Now let $\frac{1-\alpha x-\sqrt{1-2\alpha x+(\alpha^2-4\beta)x^2}}{2\beta x^2}$ be the generating function of the sequence $\{d_n\}_{n\geqslant 0}$. For convenient, let $A=-2\alpha$ and $B=\alpha^2-4\beta$. Lots of famous sequences have GF's of this form. For examples, $(\alpha,\beta)=(1,1)$ yields the Motzkin number, and $(3,9)$ as well as $(5,5)$ are associated with the numbers of Motzkin paths with multiple colors for level steps. Also $(\alpha,\beta)=(2,1)$ creates a shifted Catalan number, $(3,2)$ a shifted little Schröder number [22, A001003], and $(4,1)$ the number of walks on cubic lattice starting and finishing on the horizontal plane but never going below it [22, A005572]. For more examples, please refer to [3]. The next result can be verified by a process similar to the proof of the last theorem.

Theorem 5. *We have*

$$\sum_{k=0}^{p-1}\frac{d_k}{m^k}\equiv\frac{m^2+Am+B}{2\beta}\left(1-\left(\frac{m^2+Am+B}{p}\right)\right)+2 \pmod{p}.$$

4 Enumerating $\sum_{k=0}^{p-1-h} \frac{a_k a_{k+h}}{(\pm B)^k}$ (mod p)

Let $\{a_n\}_{n\geqslant 0}$ still associate with a generating functions of form $(1 + Ax + Bx^2)^{\frac{N}{2}}$. In this and the next sections we assume $B \not\equiv 0 \pmod p$. Given nonnegative integer h with $h \leqslant p-1$, we are interested in two summations: (S1) $\sum_{k=0}^{p-1-h} \frac{a_k a_{k+h}}{B^k}$ (mod p) and (S2) $\sum_{k=0}^{p-1-h} \frac{a_k a_{k+h}}{(-B)^k}$ (mod p). For convenience, we use $\pm B$ to denote B and $-B$ simultaneously. Let $G(x) = a_0 + a_1 x + \cdots a_{p-1}x^{p-1} \equiv (1 + Ax + Bx^2)^{\frac{N}{2}} \pmod{x^p}$ and $Q(x) = (1 + Ax + Bx^2)^{\frac{p+N}{2}} = q_0 + q_1 x + \cdots + q_{p+N}x^{p+N}$. (See (r3) for the formula of q_m.) Now we apply $[x^{-h}]G(x)G(\frac{1}{x})$ to evaluate $\sum_{k=0}^{p-1} a_k a_{k+h}$ and also use the fact $G(x) \equiv Q(x) \pmod{p, x^p}$ (see Theorem 1).

$$\begin{aligned}
\sum_{k=0}^{p-h-1} \frac{a_k a_{k+h}}{(\pm B)^k} &= [x^{-h}]G(\frac{x}{\pm B})G(\frac{1}{x}) \\
\equiv\ & [x^{-h}]Q(\frac{x}{\pm B})Q(\frac{1}{x}) - \sum_{k\geqslant p-h} \frac{q_k q_{k+h}}{(\pm B)^k} \pmod p \\
=\ & [x^{-h}]\left(1 + \frac{Ax}{\pm B} + \frac{x^2}{B}\right)^{\frac{p+N}{2}} \left(1 + \frac{A}{x} + \frac{B}{x^2}\right)^{\frac{p+N}{2}} - \sum_{k\geqslant p-h} \frac{q_k q_{k+h}}{(\pm B)^k} \\
=\ & B^{\frac{p+N}{2}}[x^{p+N-h}]\left(1 + \frac{Ax}{\pm B} + \frac{x^2}{B}\right)^{\frac{p+N}{2}} \left(1 + \frac{Ax}{B} + \frac{x^2}{B}\right)^{\frac{p+N}{2}} - \sum_{k\geqslant p-h} \frac{q_k q_{k+h}}{(\pm B)^k} \\
=\ & -\sum_{k\geqslant p-h} \frac{q_k q_{k+h}}{(\pm B)^k} + B^{\frac{p+N}{2}} \times [x^{p+N-h}] \begin{cases} (1 + \frac{A}{B}x + \frac{1}{B}x^2)^{p+N} & \text{for (S1);} \\ (1 + \frac{2B-A^2}{B^2}x^2 + \frac{1}{B^2}x^4)^{\frac{p+N}{2}} & \text{for (S2).} \end{cases} \qquad (10)
\end{aligned}$$

The first common term $\sum_{k\geqslant p-h} \frac{q_k q_{k+h}}{(\pm B)^k}$ can be avoided if and only if $N \leqslant -1$ (see (r2) and (r3)). Now the result of (S2) is ready.

Theorem 6. *The summation* $\sum_{k=0}^{p-h-1} \frac{a_k a_{k+h}}{(-B)^k}$ (mod p) *is equivalent to*

$$B^{\frac{N+1}{2}} \left(\frac{B}{p}\right) [x^{p+N-h}] \left(1 + \frac{2B - A^2}{B^2}x^2 + \frac{1}{B^2}x^4\right)^{\frac{p+N}{2}} - \sum_{k\geqslant p-h} \frac{q_k q_{k+h}}{(-B)^k} \pmod{p}.$$

Particularly, if h is odd then the first term is 0, *and if $N \leqslant -1$ then the last term is* 0.

Example 7. Let $N = -1$ and $B = 1$. For instances, $\frac{1}{\sqrt{1-6x+x^2}}$ is the GF of the central Delannoy numbers, $\frac{1}{\sqrt{1-10x+x^2}}$ is associated with the colored Delannoy paths, and $\frac{1}{\sqrt{1-14x+x^2}}$ is associated with the central coefficients of $(1 + 7x + 12x^2)$. So $\sum_{k=0}^{p-h-1}(-1)^k a_k a_{k+h} \equiv 0$ (mod p) if h is odd; otherwise let $p-h-1 = 2e$ and $\frac{p-1}{2} = M$, and then $\sum_{k=0}^{p-h-1}(-1)^k a_k a_{k+h}$ (mod p) is equivalent to

$$[x^e](1 + (2 - A^2)x + x^2)^M = \sum_{k=\lceil \frac{e}{2} \rceil}^{e} \binom{M}{M-k,\ 2k-e,\ e-k}(2 - A^2)^{2k-e}.$$

As for (S1), we continuously simplify the last term in (10) as

$$[x^{p+N-h}]\left(1+\frac{A}{B}x+\frac{1}{B}x^2\right)^N+\frac{A}{B}[x^{N-h}]\left(1+\frac{A}{B}x+\frac{1}{B}x^2\right)^N,$$

because $(1+\frac{A}{B}x+\frac{1}{B}x^2)^p \equiv 1+\frac{A}{B}x^p+\frac{1}{B}x^{2p} \pmod p$ in which x^{2p} is ignored for its exponent being too large.

Theorem 8. *Let* $(1+Ax+Bx^2)^{\frac{N}{2}}=\sum_{n\geqslant 0}a_nx^n$ *and* $(1+Ax+Bx^2)^{\frac{p+N}{2}}=\sum_{n=0}^{p+N}q_nx^n$*. Then* $\sum_{k=0}^{p-h-1}\frac{a_ka_{k+h}}{B^k} \pmod p$ *is equivalent to*

$$B^{\frac{N+1}{2}}\left(\frac{B}{p}\right)[x^{p+N-h}]\left(1+\frac{A}{B}x+\frac{1}{B}x^2\right)^N+AB^{\frac{N-1}{2}}\left(\frac{B}{p}\right)[x^{N-h}]\left(1+\frac{A}{B}x+\frac{1}{B}x^2\right)^N$$
$$-\sum_{k\geqslant p-h}\frac{q_kq_{k+h}}{B^k}.$$

Particularly, only the first term remains when $N\leqslant -1$*, the first term is zero when* $N\geqslant 1$ *and* $p>N+h$*, and the second term is zero when* $N<h$*.*

Example 9. Again, let $N=-1$ and then $\sum_{k=0}^{p-h-1}\frac{a_ka_{k+h}}{B^k} \pmod p$ is equivalent to

$$\left(\frac{B}{p}\right)[x^e](1+\frac{A}{B}x+\frac{1}{B}x^2)^{-1}=\sum_{k=\lceil\frac{e}{2}\rceil}^{e}(-1)^k\binom{k}{2k-e,\ e-k}A^{2k-e}B^{-k}$$

where $e=p-h-1$.

Since $x/(1+\frac{A}{B}x+\frac{1}{B}x^2)$ is the generating function of the Lucas sequence u_n that satisfies the second order recurrence relation

$$u_n=-\frac{A}{B}u_{n-1}-\frac{1}{B}u_{n-2},$$

with the initial $u_0=0$ and $u_1=1$, we also have

$$\begin{aligned}\sum_{k=0}^{p-h-1}\frac{a_ka_{k+h}}{B^k} &\equiv u_{p-h}\left(\frac{B}{p}\right) \pmod p\\ &= \frac{\alpha^{p-h}-\beta^{p-h}}{\alpha-\beta}\left(\frac{B}{p}\right),\end{aligned}$$

where α and β are roots of $x^2+\frac{A}{B}x+\frac{1}{B}$.

5 Summations $\sum_{k=0}^{p-2-h}\frac{b_kb_{k+h}}{(\pm B)^k}$ and $\sum_{k=0}^{p-3-h}\frac{d_kd_{k+h}}{B^k}$

We observe some applications here. Let $\frac{1-\alpha x-\sqrt{1-2\alpha x+(\alpha^2-4\beta)x^2}}{2\beta x^2}$ be the generating function of $\{d_n\}_{n\geqslant 0}$. For convenience let $A=-2\alpha$ and $B=\alpha^2-4\beta$.

Since $d_{k-2}=-\frac{a_k}{2\beta} \pmod p$ for $k=2,3,\ldots,p-1$, we have

$$\begin{aligned}\sum_{k=0}^{p-3-h}\frac{d_kd_{k+h}}{(\pm B)^k} &\equiv \frac{B^2}{4\beta^2}\sum_{k=2}^{p-1-h}\frac{a_ka_{k+h}}{(\pm B)^k} \pmod p\\ &= \frac{B^2}{4\beta^2}\left(\sum_{k=0}^{p-1-h}\frac{a_ka_{k+h}}{(\pm B)^k}-a_0a_h-\frac{a_1a_{h+1}}{\pm B}\right).\end{aligned}$$

Before we apply the formula of $\sum_{k=0}^{p-1-h}\frac{a_ka_{k+h}}{(\pm B)^k}$ given in the last section, let us recall the term $\sum_{k\geqslant p-h}\frac{q_kq_{k+h}}{(\pm B)^k}$ in both Theorems 6 and 8. With $N=1$ we have $\sum_{k\geqslant p-h}\frac{q_kq_{k+h}}{(\pm B)^k}=\frac{q_{p-h}q_p}{(\pm B)^{p-h}}+\frac{q_{p-h+1}q_{p+1}}{(\pm B)^{p-h+1}}$. Notice that, the coefficients of $(1+Ax+Bx^2)^M=q_0+q_1x+\cdots+q_{2M}x^{2M}$ have a sort of symmetric property, i.e., $B^{M-k}q_k=q_{2M-k}$ for $k=1,2,\ldots,2M$, which can be easily proved by induction on M. Let $M=\frac{p+1}{2}$ and we get

$$\begin{aligned}\frac{p_{2M-k-h}p_{2M-k}}{(\pm B)^{2M-k-h}} &= (\pm 1)^h\frac{p_kp_{k+h}}{(\pm B)^k}\\ &\equiv (\pm 1)^h\frac{a_ka_{k+h}}{(\pm B)^k} \pmod p. \qquad (11)\end{aligned}$$

Particularly, $\frac{p_{p+1-h}p_{p+1}}{(\pm B)^{p+1-h}}\equiv(\pm 1)^ha_0a_h \pmod p$ and $\frac{p_{p-h}p_p}{(\pm B)^{p-h}}\equiv(\pm 1)^h\frac{a_1a_{h+1}}{\pm B} \pmod p$. Moreover, for $N=1$ and $h\leqslant p-3$, the term $B^{\frac{N+1}{2}}\left(\frac{B}{p}\right)[x^{p+N-h}](1+\frac{A}{B}x+\frac{1}{B}x^2)^N$ in Theorem 8 must be 0. Now we derive conclusion and show some examples as follows.

Theorem 10. *The congruence* $\sum_{k=0}^{p-3-h}\frac{d_kd_{k+h}}{B^k} \pmod p$ *is equivalent to*

$$\frac{B^2}{4\beta^2}\left(A\left(\frac{B}{p}\right)[x^{1-h}]\left(1+\frac{A}{B}x+\frac{1}{B}x^2\right)-2a_0a_h-\frac{2a_1a_{1+h}}{B}\right).$$

Corollary 11. *Let* $2\leqslant h\leqslant p-3$. *We have*

$$\sum_{k=0}^{p-3-h}\frac{d_kd_{k+h}}{B^k}\equiv-\frac{B^2}{2\beta^2}\left(a_0a_h+\frac{a_1a_{1+h}}{B}\right) \pmod p,$$

which is a fixed number modulo any prime $p>2$.

Example 12. Notice that $a_0=1$, $a_1=\frac{A}{2}$, $a_2=\frac{B}{2}-\frac{A^2}{8}$, $a_3=-\frac{AB}{4}+\frac{A^3}{16}$ and $a_4=-\frac{B^2}{8}+\frac{3A^2B}{16}-\frac{5A^4}{128}$. For $h=0,1,2,3$ and $p\geqslant h+3$ we have following examples:

$$\sum_{k=0}^{p-3}\frac{{d_k}^2}{B^k} \equiv \frac{B}{8\beta^2}\left(2A^2\left(\frac{B}{p}\right)-4B-A^2\right) \pmod p,$$

$$\begin{aligned}
\sum_{k=0}^{p-4} \frac{d_k d_{k+1}}{B^k} &\equiv \frac{AB}{32\beta^2}\left(8B\left(\frac{B}{p}\right) - 12B + A^2\right) \pmod{p}, \\
\sum_{k=0}^{p-5} \frac{d_k d_{k+2}}{B^k} &\equiv -\frac{B}{64\beta^2}\left(16B^2 - 8A^2B + A^4\right) \pmod{p}, \\
\sum_{k=0}^{p-6} \frac{d_k d_{k+3}}{B^k} &\equiv \frac{5AB}{512\beta^2}\left(16B^2 - 8A^2B + A^4\right) \pmod{p}
\end{aligned}$$

Particularly, given $(A, B, \beta) = (-2, -3, 1)$ (so we need $p \neq 3$) that yields the Motzkin numbers, the four summations above are respectively equivalent to

$$-3\left(\frac{-3}{p}\right) - 3, \quad -\frac{9}{2}\left(\frac{-3}{p}\right) + \frac{15}{2}, \quad 12 \quad \text{and} \quad 15 \pmod{p}.$$

Theorem 13. *The congruence* $\sum_{k=0}^{p-3-h} \frac{d_k d_{k+h}}{(-B)^k} \pmod{p}$ *is equivalent to* 0 *if* h *is odd, and equivalent to*

$$\frac{B^2}{4\beta^2}\left(B\left(\frac{B}{p}\right)[x^{p+1-h}]\left(1 + \frac{2B - A^2}{B^2}x^2 + \frac{1}{B^2}x^4\right)^{\frac{p+1}{2}} - 2a_0a_h - 2\frac{a_1a_{1+h}}{B}\right),$$

if h *is even.*

One can refer to (r3) for the precise value of $[x^{p+1-h}]\left(1 + \frac{2B-A^2}{B^2}x^2 + \frac{1}{B^2}x^4\right)^{\frac{p+1}{2}}$.

Let $\frac{1-\alpha x-\sqrt{1-2(\alpha+\beta)x+Bx^2}}{\beta x}$ be the generating function of the sequence $\{b_n\}_{n\geqslant 0}$, and let $A = -2(\alpha + \beta)$ for convenience. Since $b_0 = 1$ and $b_{k-1} \equiv -\frac{a_k}{\beta} \pmod{p}$ for $k = 2, 3, \ldots, p-1$, we have

$$\begin{aligned}
\sum_{k=0}^{p-2-h} \frac{b_k b_{k+h}}{(\pm B)^k} &\equiv b_0 b_h + \frac{\pm B}{\beta^2}\sum_{k=2}^{p-1-h} \frac{a_k a_{k+h}}{(\pm B)^k} \pmod{p} \\
&= b_h \pm \frac{B}{\beta^2}\left(\sum_{k=0}^{p-1-h} \frac{a_k a_{k+h}}{(\pm B)^k} - a_0 a_h - \frac{a_1 a_{1+h}}{\pm B}\right).
\end{aligned}$$

This is quick similar to (11), so we can directly get

Theorem 14. *The congruence* $\sum_{k=0}^{p-2-h} \frac{b_k b_{k+h}}{B^k} \pmod{p}$ *is equivalent to*

$$b_h + \frac{B}{\beta^2}\left(A\left(\frac{B}{p}\right)[x^{1-h}](1 + \frac{A}{B}x + \frac{1}{B}x^2) - 2a_0a_h - \frac{2a_1a_{1+h}}{B}\right).$$

The congruence $\sum_{k=0}^{p-2-h} \frac{b_k b_{k+h}}{(-B)^k} \pmod{p}$ *is equivalent to* b_h *if* h *is odd, and equivalent to*

$$b_h - \frac{B}{\beta^2}\left(B\left(\frac{B}{p}\right)[x^{p+1-h}]\left(1 + \frac{2B - A^2}{B^2}x^2 + \frac{1}{B^2}x^4\right)^{\frac{p+1}{2}} - 2a_0a_h - 2\frac{a_1a_{1+h}}{B}\right),$$

if h *is even.*

6 More applications

Let $a_n = \binom{2n}{n}$ be the central binomial coefficient whose generating function is $G(x) = \frac{1}{\sqrt{1-4x}}$. We have

$$\begin{aligned}\sum_{k=0}^{p-1-h} 16^k a_k a_{k+h} &= 4^h[x^{-h}]G(x/4)G(1/4x)\\ &\equiv 4^h\left(\frac{-1}{p}\right)[x^{\frac{p-1}{2}-h}](1-x)^{p-1} \pmod p\\ &\equiv 4^h\left(\frac{-1}{p}\right)[x^{\frac{p-1}{2}-h}](1-x)^{-1} \pmod p\\ &= 4^h\left(\frac{-1}{p}\right).\end{aligned}$$

Almost same procedure can be applied on the problem $\sum_{k=0}^{p-1-h} A^{-2k}a_k a_{k+h}$ for some other a_n whose generating function is $G(x) = (1-Ax)^{\frac{N}{2}}$ for odd integer N with $|N| < p$.

In the following final example, we show an application involving two different sequences by the same technique.

Lemma 15. *Given integers* $r = \lfloor\frac{p-1}{4}\rfloor, \ldots, \frac{p-3}{2}, \frac{p-1}{2}$ *and* $0 \leqslant h \leqslant \lfloor\frac{3p+1}{4}\rfloor - 2$*, we have*

$$\sum_{k=0}^{r} 64^{-k}\binom{4k}{2k}c_{k+h} \equiv \begin{cases} 0 \pmod p & \text{if } 0 \leqslant h < \frac{p-3}{4} \text{ or } \frac{p-1}{2} < h \leqslant \lfloor\frac{3p+1}{4}\rfloor - 2;\\ 2^{2h+1}\left(\frac{-1}{p}\right)\binom{\frac{p+1}{2}}{p-1-2h} \pmod p & \text{if } \frac{p-3}{4} \leqslant h \leqslant \frac{p-1}{2}.\end{cases}$$

Proof. The sequence of the central binomial coefficients $\binom{2k}{k}$ $(k \geqslant 0)$ has GF $\frac{1}{\sqrt{1-4x}}$ that comes from the identity $\binom{2k}{k} = 4^k\binom{-1/2}{k}$. Given $t = \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-1$, we have

$$\begin{aligned}\sum_{k=0}^{t}\binom{2k}{k}\frac{x^k}{4^k} &= \sum_{k=0}^{t}\binom{-1/2}{k}x^k\\ &\equiv \sum_{k=0}^{p-1}\binom{-1/2}{k}x^k \pmod p\\ &\equiv (1-x)^{-\frac{1}{2}} \pmod{x^p}\\ &\equiv (1-x)^{\frac{p-1}{2}} \pmod{x^p, p} \text{ or } \pmod{x^{p-1}, p},\end{aligned}$$

where the equivalence on the second line dues to (ii) in Section 1. By the same reason, we can write $\pmod{x^{p-1}, p}$ additionally on the last line. And then we get

$$\sum_{k=0}^{\lfloor\frac{t}{2}\rfloor}\binom{4k}{2k}\frac{x^{2k}}{16^k} \equiv \frac{1}{2}\left((1-x)^{\frac{p-1}{2}} + (1+x)^{\frac{p-1}{2}}\right) \pmod{x^{p-1}, p}.$$

For convenience, let $t = \frac{p-1}{2}$ in the rest of the proof.

On the other hand, the sequence of the Catalan numbers c_k has GF $C(x) = \frac{1-\sqrt{1-4x}}{2x}$. Again, $c_k \equiv 0 \pmod{p}$ for $k = \frac{p+1}{2}, \dots p-2$ by (ii). So we have

$$\begin{aligned}
\sum_{k=0}^{\frac{p-1}{2}} c_k \frac{x^{-2k}}{4^k} &\equiv \sum_{k=0}^{p-2} c_k \frac{x^{-2k}}{4^k} \pmod{p} \\
&\equiv C\left(\frac{1}{4x^2}\right) \pmod{x^{p-1}} \\
&= 2x^2 - 2x^{-(p-1)}(x^2-1)^{\frac{p+1}{2}}.
\end{aligned}$$

Given $0 \leqslant h \leqslant \lfloor \frac{3p+1}{4} \rfloor - 2$ (for $\lfloor \frac{p-1}{4} \rfloor + h \leqslant p-2$ by considering the term c_{k+h}), finally we derive that

$$\begin{aligned}
\sum_{k=0}^{\lfloor \frac{p-1}{4} \rfloor} \frac{\binom{4k}{2k}}{16^k} \cdot \frac{c_{k+h}}{4^{k+h}} &\equiv [x^{-2h}] - x^{-(p-1)}(x^2-1)^{\frac{p+1}{2}} \left((1-x)^{\frac{p-1}{2}} + (1+x)^{\frac{p-1}{2}}\right) \pmod{p} \\
&\equiv [x^{p-1-2h}] \left(\frac{-1}{p}\right) (1-x^2)^{\frac{p+1}{2}} \left((1-x)^{\frac{p-1}{2}} + (1+x)^{\frac{p-1}{2}}\right) \pmod{p} \\
&= [x^{p-1-2h}] \left(\frac{-1}{p}\right) \left((1+x)^{\frac{p+1}{2}}(1-x)^p + (1+x)^p(1-x)^{\frac{p+1}{2}}\right) \\
&\equiv [x^{p-1-2h}] \left(\frac{-1}{p}\right) \left((1+x)^{\frac{p+1}{2}} + (1-x)^{\frac{p+1}{2}}\right) \pmod{p} \\
&= \begin{cases} 0 & \text{if } 0 \leqslant h < \frac{p-3}{4} \text{ or } \frac{p-1}{2} < h \leqslant \lfloor \frac{3p+1}{4} \rfloor - 2; \\ 2\left(\frac{-1}{p}\right)\binom{\frac{p+1}{2}}{p-1-2h} & \text{if } \frac{p-3}{4} \leqslant h \leqslant \frac{p-1}{2}. \end{cases}
\end{aligned}$$

We complete the proof by replacing the upper limit $\lfloor \frac{p-1}{4} \rfloor$ by any of $\lfloor \frac{p-1}{4} \rfloor, \dots, \frac{p-1}{2}$. □

References

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

[2] F. Beukers. Another congruence for the Apéry numbers. *J. Number Theory*, 25:201–210, 1987.

[3] D. Callan. On generating functions involving the square root of a quadratic polynomial. *J. Integer Seq.*, 10:Article 07.5.2, 2007.

[4] S. Chowla, J. Cowles and M. Cowles. Congruence properties of Apéry numbers. *J. Number Theory*, 12:188–190, 1980.

[5] K.S. Davis and W.A. Webb. Lucas' theorem for prime powers. *Europ. J. Combin.*, 11:229–233, 1990.

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

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

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

[9] S.-P. Eu, S.-C. Liu, and Y.-N. Yeh. On the congruences of some Combinatorial numbers. *Studies in Applied Mathematics*, 116:135–144, 2006.

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

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

[12] I.M. Gessel. Some congruences for generalized Euler numbers. *Can. J. Math.*, 35:687–709, 1983.

[13] A. Granville. Arithmetic Properties of Binomial Coefficients I: Binomial Coefficients modulo prime powers.
`http://www.cecm.sfu.ca/organics/papers/granville/Binomial/toppage.html`

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

[15] J.G. Huard, B.K. Spearman, and K.S. Williams. Pascal's triangle modulo 4. *Europ. J. Combin.*, 19:45–62, 1998.

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

[17] S.-C. Liu and J. C.-C. Yeh. Catalan numbers modulo 2^k, *J. Integer Seq.*, 13:Article 10.5.4, 2010.

[18] F. Luca and M. Klazar. On integrality and periodicity of the Motzkin numbers. *Aequationes Mathematicae*, 69:68–75, 2005.

[19] F. Lucas. Sur les congruences des numbres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un modulo premier. *Bull. Soc. Math. France*, 6:49–54, 1877–1878.

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

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

[22] N.J.A. Sloane. The On-Line Encyclopedia of Integer Sequences. `http://oeis.org`

[23] Z.-W. Sun. Binomial coefficients, Catalan numbers and Lucas quotients. *Sci. China Math.*, 53:2473–2488, 2010.

[24] Z.-W. Sun. On Delannoy numbers and Schröder numbers. *J. Number Theory*, 131:2387–2397, 2011.

[25] S. Wolfram. *A New Kind of Science*, Champaign, IL: Wolfram Media. 870 and 931–932, 2002.