Sci. China Math. 53(2010), no. 9, 2473–2488.

BINOMIAL COEFFICIENTS, CATALAN NUMBERS AND LUCAS QUOTIENTS

Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
`http://math.nju.edu.cn/∼zwsun`

Dedicated to Prof. Yuan Wang on the occasion of his 80th birthday

Abstract. Let p be an odd prime and let $a, m \in \mathbb{Z}$ with $a > 0$ and $p \nmid m$. In this paper we determine $\sum_{k=0}^{p^a-1}\binom{2k}{k+d}/m^k$ mod p^2 for $d = 0, 1$; for example,

$$\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^k} \equiv \left(\frac{m^2-4m}{p^a}\right) + \left(\frac{m^2-4m}{p^{a-1}}\right)u_{p-(\frac{m^2-4m}{p})} \pmod{p^2},$$

where $(-)$ is the Jacobi symbol and $\{u_n\}_{n\geqslant 0}$ is the Lucas sequence given by $u_0 = 0$, $u_1 = 1$ and $u_{n+1} = (m-2)u_n - u_{n-1}$ $(n = 1, 2, 3, \dots)$. As an application, we determine $\sum_{0<k<p^a,\, k\equiv r \pmod{p-1}} C_k$ modulo p^2 for any integer r, where C_k denotes the Catalan number $\binom{2k}{k}/(k+1)$. We also pose some related conjectures.

1. Introduction

The well-known Catalan numbers are given by

$$C_k = \frac{1}{k+1}\binom{2k}{k} = \binom{2k}{k} - \binom{2k}{k+1} \quad (k \in \mathbb{N} = \{0, 1, 2, \dots\}).$$

They have lots of combinatorial interpretations, see, e.g., [St, pp. 219–229].

2010 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 11A07, 11B39.

Keywords. Congruences, binomial coefficients, Catalan numbers, Lucas quotients.

Supported by the National Natural Science Foundation (grant 10871087) and the Overseas Cooperation Fund (grant 10928101) of China.

Let p be a prime. In 2006 H. Pan and Z. W. Sun [PS] obtained some congruences involving Catalan numbers; for example, (1.16) in [PS] yields

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

where $(-)$ is the Jacobi symbol. In a recent paper [ST1] Sun and Tauraso investigated $\sum_{k=0}^{p^a-1}\binom{2k}{k+d}/m^k$ and $\sum_{k=1}^{p-1}\binom{2k}{k+d}/(km^{k-1})$ modulo p via Lucas sequences, where d is an integer among $0,\ldots,p^a$ and m is an integer not divisible by p. By Sun and R. Tauraso [ST2, Corollary 1.1], for any $a \in \mathbb{Z}^+ = \{1,2,3,\ldots\}$ we have

$$\sum_{k=0}^{p^a-1}\binom{2k}{k} \equiv \left(\frac{p^a}{3}\right) \pmod{p^2} \tag{1.1}$$

and

$$\sum_{k=0}^{p^a-1}\binom{2k}{k+1} \equiv \left(\frac{p^a-1}{3}\right) - p\delta_{p,3} \pmod{p^2}, \tag{1.2}$$

where the Kronecker symbol $\delta_{m,n}$ takes 1 or 0 according as $m=n$ or not.

Let $A \in \mathbb{Z}$ and $B \in \mathbb{Z}\setminus\{0\}$. The Lucas sequences $u_n = u_n(A,B)$ $(n \in \mathbb{N})$ and $v_n = v_n(A,B)$ $(n \in \mathbb{N})$ are defined as follows:

$$u_0 = 0,\ u_1 = 1,\ \text{and}\ u_{n+1} = Au_n - Bu_{n-1}\ (n = 1,2,3,\ldots)$$

and

$$v_0 = 2,\ v_1 = A,\ \text{and}\ v_{n+1} = Av_n - Bv_{n-1}\ (n = 1,2,3,\ldots).$$

The characteristic equation $x^2 - Ax + B = 0$ has two roots

$$\alpha = \frac{A+\sqrt{\Delta}}{2} \quad \text{and} \quad \beta = \frac{A-\sqrt{\Delta}}{2},$$

where $\Delta = A^2 - 4B$. By induction, one can easily get the following well-known formulae:

$$(\alpha-\beta)u_n = \alpha^n - \beta^n \quad \text{and} \quad v_n = \alpha^n + \beta^n.$$

In the case $\alpha = \beta$ (i.e., $\Delta = 0$), clearly $u_n = n(A/2)^{n-1}$ for all $n \in \mathbb{Z}^+$. If p is an odd prime not dividing B, then it is known that $p \mid u_{p-(\frac{\Delta}{p})}$ (see, e.g., [S06]), and we call the integer $u_{p-(\frac{\Delta}{p})}/p$ a *Lucas quotient*. There are many congruences for some special Lucas quotients such as Fibonacci quotients and Pell quotients. (Cf. [SS] and [S02].)

In this paper we establish the following general theorem which includes some previous congruences as special cases and relates binomial coefficients to Lucas quotients.

Theorem 1.1. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. Let m be any integer not divisible by p and set $\Delta = m(m-4)$. Then we have*

$$\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k}}{m^k} \equiv \left(\frac{\Delta}{p^a}\right) + \left(\frac{\Delta}{p^{a-1}}\right) u_{p-(\frac{\Delta}{p})}(m-2,1) \pmod{p^2} \tag{1.3}$$

and

$$\begin{aligned}\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k+1}}{m^k} \equiv\ & 1 - m^{p-1} + \left(\frac{m}{2}-1\right)\left(\left(\frac{\Delta}{p^a}\right)-1\right) \\ & + \left(\frac{m}{2}-1\right)\left(\frac{\Delta}{p^{a-1}}\right) u_{p-(\frac{\Delta}{p})}(m-2,1) \pmod{p^2}.\end{aligned} \tag{1.4}$$

Consequently,

$$\begin{aligned}&\sum_{k=1}^{p^a-1} \frac{\binom{2k+1}{k}}{m^k} + m^{p-1} - 1 \\ \equiv & \frac{m}{2}\left(\left(\frac{\Delta}{p^a}\right) - 1 + \left(\frac{\Delta}{p^{a-1}}\right) u_{p-(\frac{\Delta}{p})}(m-2,1)\right) \pmod{p^2}\end{aligned} \tag{1.5}$$

and

$$\begin{aligned}\sum_{k=1}^{p^a-1} \frac{C_k}{m^k} \equiv & m^{p-1} - 1 - \frac{m-4}{2}\left(\left(\frac{\Delta}{p^a}\right)-1\right) \\ & - \frac{m-4}{2}\left(\frac{\Delta}{p^{a-1}}\right) u_{p-(\frac{\Delta}{p})}(m-2,1) \pmod{p^2}.\end{aligned} \tag{1.6}$$

Here is a consequence of Theorem 1.1.

Corollary 1.1. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k}}{2^k} \equiv (-1)^{(p^a-1)/2} \pmod{p^2} \ \textit{and} \ \sum_{k=1}^{p^a-1} \frac{\binom{2k}{k+1}}{2^k} \equiv 1 - 2^{p-1} \pmod{p^2}.$$

Also,

$$\sum_{k=1}^{p^a-1} \frac{\binom{2k}{k+1}}{4^k} \equiv p\delta_{a,1} - 4^{p-1} \pmod{p^2} \ \textit{and} \ \sum_{k=1}^{p^a-1} \frac{C_k}{4^k} \equiv 2^p - 2 \pmod{p^2}.$$

If $p \neq 3$ then

$$\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k}}{3^k} \equiv \left(\frac{p^a}{3}\right) \pmod{p^2} \ \textit{and} \ \sum_{k=1}^{p^a-1} \frac{C_k}{3^k} \equiv 3^{p-1} - 1 + \frac{(\frac{p^a}{3}) - 1}{2} \pmod{p^2}.$$

When $p\neq 5$ we have

$$\sum_{k=0}^{p^a-1}(-1)^k\binom{2k}{k}\equiv\left(\frac{p^a}{5}\right)\left(1-2F_{p-(\frac{p}{5})}\right)\pmod{p^2},$$

$$\sum_{k=1}^{p^a-1}(-1)^kC_k\equiv\frac{5}{2}\left(\left(\frac{p^a}{5}\right)-1\right)-5\left(\frac{p^a}{5}\right)F_{p-(\frac{p}{5})}\pmod{p^2},$$

$$\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{5^k}\equiv\left(\frac{p^a}{5}\right)\left(1+2F_{p-(\frac{p}{5})}\right)\pmod{p^2},$$

$$\sum_{k=1}^{p^a-1}\frac{C_k}{5^k}\equiv\frac{1-(\frac{p^a}{5})}{2}-\left(\frac{p^a}{5}\right)F_{p-(\frac{p}{5})}\pmod{p^2},$$

where $\{F_n\}_{n\geqslant 0}$ is the well-known Fibonacci sequence defined by

$$F_0=0,\ F_1=1,\ \text{and}\ F_{n+1}=F_n+F_{n-1}\ (n=1,2,3,\ldots).$$

Remark 1.1. (i) There is a closed formula for the sum $\sum_{k=0}^n\binom{2k}{k}/4^k$. In fact, $\binom{2k}{k}=(-4)^k\binom{-1/2}{k}$ for $k\in\mathbb{N}$ and hence

$$\sum_{k=0}^n\frac{\binom{2k}{k}}{4^k}=(-1)^n\sum_{k=0}^n\binom{-1}{n-k}\binom{-1/2}{k}=(-1)^n\binom{-3/2}{n}=\frac{2n+1}{4^n}\binom{2n}{n}$$

by the Chu-Vandermonde identity

$$\sum_{k=0}^n\binom{x}{k}\binom{y}{n-k}=\binom{x+y}{n}$$

(see, e.g., [GKP, p. 169]).

(ii) In [ST1] the authors conjectured that if $p\neq 2,5$ is a prime and $a\in\mathbb{Z}^+$ then

$$\sum_{k=0}^{p^a-1}(-1)^k\binom{2k}{k}\equiv\left(\frac{p^a}{5}\right)\left(1-2F_{p^a-(\frac{p^a}{5})}\right)\pmod{p^3}.$$

(Note that $F_{p^a-(\frac{p^a}{5})}\equiv F_{p-(\frac{p}{5})}\pmod{p^2}$ by Lemma 2.3.) This seems difficult. Those primes $p>5$ satisfying $p^2\mid F_{p-(\frac{p}{5})}$ are called Wall-Sun-Sun primes (cf. [CP, p. 32]). Up to now none of this kind of primes has been found though it is conjectured that there should be infinitely many Wall-Sun-Sun primes.

By Corollary 1.1, if p is an odd prime then

$$\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{2^k}\equiv(-1)^{(p-1)/2}\pmod{p^2}.$$

This seems to be a new characterization of odd primes and we have verified our following conjecture for $n<10^4$ via `Mathematica`.

Conjecture 1.1. *If an odd integer $n > 1$ satisfies the congruence*

$$\sum_{k=0}^{n-1} \frac{\binom{2k}{k}}{2^k} \equiv (-1)^{(n-1)/2} \pmod{n^2},$$

then n must be a prime.

As an application of Theorem 1.1, we will determine the sums

$$\sum_{\substack{0<k<p^a \\ k\equiv r \,(\mathrm{mod}\ p-1)}} \binom{2k}{k}, \quad \sum_{\substack{0<k<p^a \\ k\equiv r \,(\mathrm{mod}\ p-1)}} \binom{2k}{k+1}, \quad \sum_{\substack{0<k<p^a \\ k\equiv r \,(\mathrm{mod}\ p-1)}} C_k$$

modulo p^2 for any prime p and integers $a > 0$ and r. By (1.1) and (1.2), for $d = 0, 1$ we have

$$\sum_{k=0}^{p^a-1} \binom{2k}{k+d} \equiv \left(\frac{p^a-d}{3}\right) - p\delta_{d,1}\delta_{p,3} \pmod{p^2}.$$

Thus the task for $p = 2$ is easy; for example,

$$\begin{aligned}\sum_{\substack{0<k<2^a \\ k\equiv r \,(\mathrm{mod}\ 2-1)}} C_k &= \sum_{k=1}^{2^a-1} C_k = \sum_{k=1}^{2^a-1} \binom{2k}{k} - \sum_{k=1}^{2^a-1} \binom{2k}{k+1} \\ &\equiv \left(\frac{2^a}{3}\right) - 1 - \left(\frac{2^a-1}{3}\right) \equiv \begin{cases} 1 \pmod{2^2} & \text{if } 2 \nmid a, \\ 0 \pmod{2^2} & \text{if } 2 \mid a. \end{cases}\end{aligned}$$

So we will only handle the main case $p \neq 2$.

Theorem 1.2. *Let p be an odd prime and let $a \in \mathbb{Z}^+$.*

(i) *If a is odd and $r \in \{1, \ldots, p-1\}$, then*

$$\sum_{\substack{0<k<p^a \\ k\equiv r \,(\mathrm{mod}\ p-1)}} \binom{2k}{k+d} \equiv \binom{2r}{r+d} \pmod{p^2} \quad \text{for } d = 0, 1, \tag{1.7}$$

and also

$$\sum_{\substack{0<k<p^a \\ k\equiv r \,(\mathrm{mod}\ p-1)}} C_k \equiv C_r \pmod{p^2}. \tag{1.8}$$

(ii) *Suppose that a is even. Then, for $r = 1, \ldots, p$ we have*

$$\sum_{\substack{0<k<p^a \\ k\equiv r \,(\mathrm{mod}\ p-1)}} \binom{2k}{k} \equiv 4^r \left(1 + \frac{p}{2} + r(2^{p-1}-1)\right) - pR_p(r) \pmod{p^2}, \tag{1.9}$$

where

$$R_p(r)=\begin{cases}\sum_{s=0}^{(p-1)/2-r}\binom{2r+2s}{r+s}/((2s+1)\binom{2s}{s}) & \text{if } 0<r\leqslant (p-1)/2,\\ 0 & \text{otherwise.}\end{cases}$$

Also, if $r\in\{1,\ldots,p-1\}$ *then*

$$\begin{aligned}\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2k}{k+1}\equiv&4^r\left(1+\frac{p}{2}+(r+2)(2^{p-1}-1)\right)\\ &+p\left(R_p(r)-\frac{R_p(r+1)}{2}\right)\ (\mathrm{mod}\ p^2)\end{aligned}\tag{1.10}$$

and

$$\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}C_k\equiv 4^r(2-2^p)-p\left(2R_p(r)-\frac{R_p(r+1)}{2}\right)\ (\mathrm{mod}\ p^2).\tag{1.11}$$

In particular,

$$\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}C_k\equiv 4^r(2-2^p)\ (\mathrm{mod}\ p^2)\quad \text{for } r=\frac{p+1}{2},\ldots,p-1.\tag{1.12}$$

Remark 1.2. If p is an odd prime and $a\in\mathbb{Z}^+$ is even, then by (1.11) we have

$$\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}C_k\equiv 0\ (\mathrm{mod}\ p)\quad\text{for all } r\in\mathbb{Z}.$$

The author would like to see any combinatorial interpretation for this.

Corollary 1.2. *Let* p *be an odd prime and let* $a\in\mathbb{Z}^+$. *Then*

$$\sum_{\substack{0<k<p^a\\ k\equiv 0\,(\mathrm{mod}\ p-1)}}C_k\equiv\begin{cases}-2p-1\ (\mathrm{mod}\ p^2) & \text{if } 2\nmid a,\\ 2-2^p\ (\mathrm{mod}\ p^2) & \text{if } 2\mid a;\end{cases}\tag{1.13}$$

$$\sum_{\substack{0<k<p^a\\ k\equiv 1\ (\mathrm{mod}\ p-1)}}C_k\equiv\begin{cases}1\ (\mathrm{mod}\ p^2) & \text{if } 2\nmid a,\\ 4(2-2^p)+2p\ (\mathrm{mod}\ p^2) & \text{if } 2\mid a;\end{cases}\tag{1.14}$$

and

$$\sum_{\substack{0<k<p^a\\ k\equiv (p-1)/2\,(\mathrm{mod}\ p-1)}}C_k\equiv\begin{cases}(-1)^{(p-1)/2}2(2^p-p-1)\ (\mathrm{mod}\ p^2) & \text{if } 2\nmid a,\\ 2-2^p+(-1)^{(p+1)/2}2p\ (\mathrm{mod}\ p^2) & \text{if } 2\mid a.\end{cases}\tag{1.15}$$

Now we pose some new conjectures.

Conjecture 1.2. *Let p be any prime and let r be an integer. For $a \in \mathbb{N}$ define*

$$S_r(p^a) = \sum_{\substack{0<k<p^a \\ k\equiv r \pmod{p-1}}} C_k.$$

Then, for any $a \in \mathbb{N}$ we have

$$S_r(p^{a+2}) \equiv S_r(p^a) \pmod{p^{(1+\delta_{p,2})(a+1)}}.$$

Furthermore,

$$\frac{S_r(p^{a+2}) - S_r(p^a)}{p^{(1+\delta_{p,2})(a+1)}} + p(\delta_{p^a,2} + \delta_{p^a,3}) \mod p^2$$

does not depend on $a \in \mathbb{Z}^+$.

Conjecture 1.3. *Let p be a prime, and let $d \in \{0, \ldots, p\}$ and $r \in \mathbb{Z}$. For $a \in \mathbb{N}$ define*

$$T_r^{(d)}(p^a) = \sum_{\substack{0<k<p^a \\ k\equiv r \pmod{p-1}}} \binom{2k}{k+d}.$$

Then, for any $a \in \mathbb{N}$ we have

$$T_r^{(d)}(p^{a+2}) \equiv T_r^{(d)}(p^a) \pmod{p^a};$$

furthermore

$$\frac{T_r^{(d)}(p^{a+2}) - T_r^{(d)}(p^a)}{p^a} \mod p$$

does not depend on $a \in \mathbb{Z}^+$. If $a \in \mathbb{N}$ and $d < p = 2$, then

$$T_r^{(d)}(2^{a+2}) \equiv T_r^{(d)}(2^a) \pmod{2^{2a+2+\delta_{d,0}(1-\delta_{a,0})}}.$$

If $a \in \mathbb{Z}^+$, $d \in \{0,1\}$ and $p = 3$, then

$$T_r^{(d)}(3^{a+2}) \equiv T_r^{(d)}(3^a) \pmod{3^{a+1+\delta_{d,1}(1-\delta_{a,1})}}.$$

Given a positive integer h, two kinds of Catalan numbers of order h are defined as follows:

$$C_k^{(h)} = \frac{1}{hk+1}\binom{(h+1)k}{k} = \binom{(h+1)k}{k} - h\binom{(h+1)k}{k-1} \quad (k \in \mathbb{N})$$

and

$$\bar{C}_k^{(h)} = \frac{h}{k+1}\binom{(h+1)k}{k} = h\binom{(h+1)k}{k} - \binom{(h+1)k}{k+1} \quad (k \in \mathbb{N}).$$

In [ZPS] and [S09], the authors gave various congruences involving higher-order Catalan numbers. In particular, Sun [S09] proved that for any prime $p>3$ and $a\in\mathbb{Z}^+$ with $6\mid a$ we have the congruence

$$\sum_{\substack{0<k<p^a\\ k\equiv r\ (\mathrm{mod}\ p-1)}}\binom{3k}{k+d}\equiv 2^{d+3-2r}3^{3r-2}\pmod p$$

for all $d\in\{0,\pm1\}$ and $r\in\mathbb{Z}$; consequently,

$$\sum_{\substack{0<k<p^a\\ k\equiv r\ (\mathrm{mod}\ p-1)}}C_k^{(2)}\equiv\sum_{\substack{0<k<p^a\\ k\equiv r\ (\mathrm{mod}\ p-1)}}\bar{C}_k^{(2)}\equiv 0\pmod p$$

for any $r\in\mathbb{Z}$.

Here is our conjecture involving Catalan numbers of order 2.

Conjecture 1.4. *Let p be any prime, and set*

$$C(p^a)=\sum_{\substack{0<k<p^a\\ k\equiv 0\ (\mathrm{mod}\ p-1)}}C_k^{(2)}\ \text{ and }\ \bar{C}(p^a)=\sum_{\substack{0<k<p^a\\ k\equiv 0\ (\mathrm{mod}\ p-1)}}\bar{C}_k^{(2)}\quad\text{for } a\in\mathbb{Z}^+.$$

Then we have

$$C(p^a)\equiv\begin{cases}0\pmod p & \text{if } a\equiv 0\pmod 6,\\ \delta_{p,2}\pmod p & \text{if } a\equiv 1\pmod 6,\\ -((\frac{p}{3})+1)/2\pmod p & \text{if } a\equiv 2\pmod 6,\\ ((\frac{p}{3})-1)/2+\delta_{p,2}\pmod p & \text{if } a\equiv 3\pmod 6,\\ (1-(\frac{p}{3}))/2\pmod p & \text{if } a\equiv 4\pmod 6,\\ \delta_{p,2}-1\pmod p & \text{if } a\equiv 5\pmod 6;\end{cases}$$

and

$$\bar{C}(p^a)\equiv\begin{cases}0\pmod p & \text{if } a\equiv 0\pmod 6,\\ -2+\delta_{p,2}\pmod p & \text{if } a\equiv \pm1\pmod 6,\\ -1-2(\frac{p}{3})\pmod p & \text{if } a\equiv \pm2\pmod 6,\\ 2(\frac{p}{3})-1+\delta_{p,2}\pmod p & \text{if } a\equiv 3\pmod 6.\end{cases}$$

We will prove Theorem 1.1 and Corollary 1.1 in Section 2, and show Theorem 1.2 and Corollary 1.2 in Section 3.

2. Proof of Theorem 1.1

Lemma 2.1. *Let p be a prime and let $a, m \in \mathbb{Z}$ with $a > 0$ and $p \nmid m$. Then*

$$\sum_{k=1}^{p^a-1} \frac{\binom{2k}{k+1}}{m^k} + (m^{p-1} - 1) \equiv \frac{m-2}{2} \sum_{k=1}^{p^a-1} \frac{\binom{2k}{k}}{m^k} + p\delta_{p,2} \pmod{p^2}. \tag{2.1}$$

Proof. Observe that

$$\begin{aligned}\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k} + \binom{2k}{k+1}}{m^k} =& \frac{1}{2} \sum_{k=0}^{p^a-1} \frac{\binom{2(k+1)}{k+1}}{m^k} = \frac{1}{2} \sum_{k=1}^{p^a} \frac{\binom{2k}{k}}{m^{k-1}} \\ =& \frac{1}{2} \left(\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k}}{m^{k-1}} - m + \frac{\binom{2p^a}{p^a}}{m^{p^a-1}} \right) \\ =& \frac{m}{2} \sum_{k=0}^{p^a-1} \frac{\binom{2k}{k}}{m^k} - \frac{m}{2} + \frac{\binom{2p^a-1}{p^a-1}}{m^{p^a-1}}.\end{aligned}$$

Clearly we have

$$\begin{aligned}&\binom{2p^a-1}{p^a-1} = \prod_{k=1}^{p^a-1} \left(1 + \frac{p^a}{k}\right) \\ \equiv& 1 + \frac{1}{2} \sum_{k=1}^{p^a-1} \left(\frac{p^a}{k} + \frac{p^a}{p^a-k} \right) \equiv 1 + p\delta_{p,2} \pmod{p^2}.\end{aligned}$$

(See also [ST2, Lemma 2.2].) Note that

$$\frac{1}{m^{p^a-1}} \equiv \frac{1}{m^{p-1}} \equiv 2 - m^{p-1} \pmod{p^2}$$

since $m^{p(p-1)} \equiv 1 \pmod{p^2}$ and $(m^{p-1}-1)^2 \equiv 0 \pmod{p^2}$ by Euler's theorem and Fermat's little theorem. Therefore

$$\begin{aligned}\sum_{k=1}^{p^a-1} \frac{\binom{2k}{k+1}}{m^k} \equiv& \left(\frac{m}{2} - 1\right) \sum_{k=1}^{p^a-1} \frac{\binom{2k}{k}}{m^k} + 1 - m^{p-1} + p\delta_{p,2}(2 - m^{p-1}) \\ \equiv& \frac{m-2}{2} \sum_{k=1}^{p^a-1} \frac{\binom{2k}{k}}{m^k} + 1 - m^{p-1} + p\delta_{p,2} \pmod{p^2}.\end{aligned}$$

This concludes the proof. □

Lemma 2.2. *Let p be any prime and let $a\in\mathbb{Z}^+$. Let m ba an integer not divisible by p. Then*

$$\frac{m^{p-1}}{2}\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^k}+\frac{u_{p^a}(m-2,1)}{2}\equiv u_{p^a}(m,m)\ (\mathrm{mod}\ p^2). \tag{2.2}$$

Proof. By [ST1, Theorem 2.1],

$$\sum_{k=0}^{p^a-1}\binom{2k}{k}m^{p^a-1-k}=\sum_{k=0}^{p^a-1}\binom{2p^a}{k}u_{p^a-k}(m-2,1).$$

For $k\in\{1,\ldots,p^a-1\}$, clearly

$$\binom{2p^a-1}{k-1}=\prod_{0<j<k}\frac{2p^a-j}{j}\equiv\prod_{0<j<k}\frac{p^a-j}{j}=\binom{p^a-1}{k-1}\ (\mathrm{mod}\ p)$$

and hence

$$\frac{1}{2}\binom{2p^a}{k}=\frac{p^a}{k}\binom{2p^a-1}{k-1}\equiv\frac{p^a}{k}\binom{p^a-1}{k-1}=\binom{p^a}{k}\ (\mathrm{mod}\ p^2).$$

Therefore

$$\begin{aligned}&\frac{m^{p^a-1}}{2}\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^k}+\frac{u_{p^a}(m-2,1)}{2}\\ =&\frac{1}{2}\sum_{k=1}^{p^a-1}\binom{2p^a}{k}u_{p^a-k}(m-2,1)+u_{p^a}(m-2,1)\\ \equiv&\sum_{k=1}^{p^a}\binom{p^a}{k}u_{p^a-k}(m-2,1)+u_{p^a}(m-2,1)\\ \equiv&\sum_{j=0}^{p^a}\binom{p^a}{j}u_j(m-2,1)\ (\mathrm{mod}\ p^2).\end{aligned}$$

If $\Delta=(m-2)^2-4=m^2-4m\neq 0$ then

$$\begin{aligned}&\sum_{j=0}^{p^a}\binom{p^a}{j}u_j(m-2,1)\\ =&\sum_{j=0}^{p^a}\binom{p^a}{j}\frac{1}{\sqrt{\Delta}}\left(\left(\frac{m-2+\sqrt{\Delta}}{2}\right)^j-\left(\frac{m-2-\sqrt{\Delta}}{2}\right)^j\right)\\ =&\frac{1}{\sqrt{\Delta}}\left(\left(\frac{m+\sqrt{\Delta}}{2}\right)^{p^a}-\left(\frac{m-\sqrt{\Delta}}{2}\right)^{p^a}\right)=u_{p^a}(m,m).\end{aligned}$$

In the case $\Delta = 0$ (i.e., $m = 4$), we have

$$\sum_{j=0}^{p^a}\binom{p^a}{j}u_j(2,1) = \sum_{j=0}^{p^a}\binom{p^a}{j}j = p^a\sum_{j=1}^{p^a}\binom{p^a-1}{j-1} = p^a2^{p^a-1} = u_{p^a}(4,4).$$

In view of the above, it suffices to show that

$$\frac{m^{p^a-1}-m^{p-1}}{2} \equiv 0 \pmod{p^2}. \tag{2.3}$$

This follows from Euler's theorem when $p \neq 2$. If $p = 2$, then (2.3) holds since $2 \nmid m$ and $m^p = m^2 \equiv 1 \pmod{2^3}$. We are done. $\square$

Now we need a lemma on Lucas sequences.

Lemma 2.3. *Let p be a prime, and let $a \in \mathbb{Z}^+$ and $A, B \in \mathbb{Z}$. Then*

$$v_{p^a}(A,B) \equiv v_{p^{a-1}}(A,B) \pmod{p^a}. \tag{2.4}$$

If $p \neq 2$, then

$$u_{p^a}(A,B) \equiv \left(\frac{\Delta}{p}\right)u_{p^{a-1}}(A,B) \pmod{p^a}, \tag{2.5}$$

where $\Delta = A^2 - 4B$. When $p \nmid 2B\Delta$, we have

$$u_{p^a-(\frac{\Delta}{p^a})}(A,B) \equiv \begin{cases} B^{((\frac{\Delta}{p^{a-1}})-(\frac{\Delta}{p^a}))/2}(\frac{\Delta}{p})u_{p^{a-1}-(\frac{\Delta}{p^{a-1}})}(A,B) \pmod{p^a} \\ B^{((\frac{\Delta}{p})-(\frac{\Delta}{p^a}))/2}(\frac{\Delta}{p^{a-1}})u_{p-(\frac{\Delta}{p})}(A,B) \pmod{p^2} \\ 0 \pmod{p} \end{cases} \tag{2.6}$$

and

$$v_{p^a-(\frac{\Delta}{p^a})}(A,B) \equiv \begin{cases} B^{((\frac{\Delta}{p^{a-1}})-(\frac{\Delta}{p^a}))/2}v_{p^{a-1}-(\frac{\Delta}{p^{a-1}})}(A,B) \pmod{p^a} \\ B^{((\frac{\Delta}{p})-(\frac{\Delta}{p^a}))/2}v_{p-(\frac{\Delta}{p})}(A,B) \pmod{p^2} \\ 2B^{(1-(\frac{\Delta}{p^a}))/2} \pmod{p}. \end{cases} \tag{2.7}$$

Proof. For convenience we let $u_n = u_n(A,B)$ and $v_n = v_n(A,B)$ for all $n \in \mathbb{N}$. We split our proof into several steps.

(i) By a known result of W. Jänichen [J] (see also [Sm] and [V]), if $\prod_{j=1}^{m}(x-\alpha_j) \in \mathbb{Z}[x]$ then

$$\alpha_1^{p^a} + \cdots + \alpha_m^{p^a} \equiv \alpha_1^{p^{a-1}} + \cdots + \alpha_m^{p^{a-1}} \pmod{p^a}.$$

Thus

$$v_{p^a} = \alpha^{p^a} + \beta^{p^a} \equiv \alpha^{p^{a-1}} + \beta^{p^{a-1}} = v_{p^{a-1}} \pmod{p^a},$$

where α and β be the two roots of the equation $x^2 - Ax + B = 0$ in the complex field.

(ii) Now we prove that $p^a \mid u_{p^a}$ under the condition $p \mid \Delta$.

If $\Delta = 0$ (i.e., $\alpha = \beta$), then A is even and $u_n = n(A/2)^{n-1}$ for all $n \in \mathbb{Z}^+$, in particular $u_{p^a} \equiv 0 \pmod{p^a}$.

Assume $\Delta \neq 0$. If $p \neq 2$, then

$$u_p \equiv u_p\left(A, \frac{A^2}{4}\right) = p\left(\frac{A}{2}\right)^{p-1} \equiv 0 \pmod{p}.$$

When $p = 2$, we have $2 \mid A$ since $p \mid \Delta$, hence $u_2 = A \equiv 0 \pmod{2}$. So we always have $p \mid u_p$. Observe that

$$\begin{aligned} u_{p^{a+1}} =& \frac{\alpha^{p^{a+1}} - \beta^{p^{a+1}}}{\alpha - \beta} \\ =& \frac{\alpha^{p^a} - \beta^{p^a}}{\alpha - \beta} \sum_{k=0}^{p-1} (\alpha^{p^a})^k (\beta^{p^a})^{p-1-k} \\ =& u_{p^a} \sum_{k=0}^{p-1} (\alpha^k \beta^{p-1-k})^{p^a} \end{aligned}$$

and

$$\begin{aligned} \sum_{k=0}^{p-1} (\alpha^k \beta^{p-1-k})^{p^a} \equiv& \bigg(\sum_{k=0}^{p-1} \alpha^k \beta^{p-1-k}\bigg)^{p^a} \\ \equiv& \left(\frac{\alpha^p - \beta^p}{\alpha - \beta}\right)^{p^a} = u_p^{p^a} \equiv 0 \pmod{p}. \end{aligned}$$

Thus, if $p^a \mid u_{p^a}$ then $p^{a+1} \mid u_{p^{a+1}}$. This concludes our induction proof of the desired congruence $u_{p^a} \equiv 0 \pmod{p^a}$.

(iii) Suppose $p \neq 2$. Now we show that

$$u_{p^a} \equiv \left(\frac{\Delta}{p^a}\right) \pmod{p}.$$

By part (ii), this holds when $p \mid \Delta$. In the case $p \nmid \Delta$, since

$$\Delta u_{p^a} = (\alpha - \beta)^2 u_{p^a} = (\alpha - \beta)(\alpha^{p^a} - \beta^{p^a}) \equiv (\alpha - \beta)^{p^a + 1} = \Delta^{(p^a+1)/2} \pmod{p},$$

we have

$$u_{p^a} \equiv \Delta^{(p^a-1)/2} \equiv \left(\frac{\Delta}{p}\right)^{\sum_{i=0}^{a-1} p^i} = \left(\frac{\Delta}{p}\right)^a = \left(\frac{\Delta}{p^a}\right) \pmod p.$$

(iv) Assume that $p \neq 2$. By part (ii), (2.5) holds when $p \mid \Delta$. Suppose $p \nmid \Delta$. In view of part (iii),

$$u_{p^a} + \left(\frac{\Delta}{p}\right) u_{p^{a-1}} \equiv 2\left(\frac{\Delta}{p^a}\right) \not\equiv 0 \pmod p.$$

For any $n \in \mathbb{N}$ we have

$$v_n^2 - \Delta u_n^2 = (\alpha^n + \beta^n)^2 - (\alpha^n - \beta^n)^2 = 4(\alpha\beta)^n = 4B^n.$$

Thus

$$\Delta(u_{p^a}^2 - u_{p^{a-1}}^2) = v_{p^a}^2 - 4B^{p^a} - (v_{p^{a-1}}^2 - 4B^{p^{a-1}})$$

and hence

$$\begin{aligned}&\Delta\left(u_{p^a} + \left(\frac{\Delta}{p}\right)u_{p^{a-1}}\right)\left(u_{p^a} - \left(\frac{\Delta}{p}\right)u_{p^{a-1}}\right)\\ =&\left(v_{p^a} + v_{p^{a-1}}\right)\left(v_{p^a} - v_{p^{a-1}}\right) - 4(B^{p^a} - B^{p^{a-1}})\\ \equiv&0 \pmod{p^a} \quad \text{(by (2.4) and Euler's theorem).}\end{aligned}$$

So (2.5) follows, for, $\Delta(u_{p^a} + (\frac{\Delta}{p})u_{p^{a-1}})$ is relatively prime to p.

(v) By induction, for $\varepsilon \in \{\pm 1\}$ and $n \in \mathbb{Z}^+$ we have

$$Au_n + \varepsilon v_n = 2B^{(1-\varepsilon)/2}u_{n+\varepsilon} \quad \text{and} \quad Av_n + \varepsilon\Delta u_n = 2B^{(1-\varepsilon)/2}v_{n+\varepsilon}. \tag{2.8}$$

Therefore, if $p \nmid 2B\Delta$ then

$$\begin{aligned}u_{p^a-(\frac{\Delta}{p^a})} =& \frac{Au_{p^a} - (\frac{\Delta}{p^a})v_{p^a}}{2B^{(1+(\frac{\Delta}{p^a}))/2}}\\ \equiv&\frac{A(\frac{\Delta}{p})u_{p^{a-1}} - (\frac{\Delta}{p^a})v_{p^{a-1}}}{2B^{(1+(\frac{\Delta}{p^a}))/2}}\\ \equiv&\left(\frac{\Delta}{p}\right)B^{((\frac{\Delta}{p^{a-1}})-(\frac{\Delta}{p^a}))/2}u_{p^{a-1}-(\frac{\Delta}{p^{a-1}})} \pmod{p^a}\end{aligned}$$

and

$$\begin{aligned}v_{p^a-(\frac{\Delta}{p^a})} =& \frac{Av_{p^a} - (\frac{\Delta}{p^a})\Delta u_{p^a}}{2B^{(1+(\frac{\Delta}{p^a}))/2}}\\ \equiv&\frac{Av_{p^{a-1}} - (\frac{\Delta}{p^{a-1}})\Delta u_{p^{a-1}}}{2B^{(1+(\frac{\Delta}{p^a}))/2}} = B^{((\frac{\Delta}{p^{a-1}})-(\frac{\Delta}{p^a}))/2}v_{p^{a-1}-(\frac{\Delta}{p^{a-1}})} \pmod{p^a}.\end{aligned}$$

Note that $u_{p^0-(\frac{\Delta}{p^0})} = u_0 = 0$ and $v_{p^0-(\frac{\Delta}{p^0})} = v_0 = 2$. So both (2.6) and (2.7) hold when $p \nmid 2B\Delta$.

So far we have completed the proof of Lemma 2.3. $\square$

Using Lemma 2.3 we can deduce the following result.

Lemma 2.4. *Let p be an odd prime, and let $a, m \in \mathbb{Z}$ with $a > 0$ and $p \nmid m$. Set $\Delta = m^2 - 4m$. Then*

$$2u_{p^a}(m,m) - u_{p^a}(m-2,1) \equiv \left(\frac{\Delta}{p^a}\right) m^{p-1} + u_{p^a - (\frac{\Delta}{p^a})}(m-2,1) \pmod{p^2}. \tag{2.9}$$

Proof. By Lemma 2,3,

$$2u_{p^a}(m,m) - u_{p^a}(m-2,1) \equiv \left(\frac{\Delta}{p^{a-1}}\right)(2u_p(m,m) - u_p(m-2,1)) \pmod{p^2}$$

and

$$u_{p^a - (\frac{\Delta}{p^a})}(m-2,1) \equiv \left(\frac{\Delta}{p^{a-1}}\right) u_{p-(\frac{\Delta}{p})}(m-2,1) \pmod{p^2}.$$

So, it suffices to prove (2.9) in the case $a = 1$.

Let α and β be the two roots of the equation $x^2 - mx + m = 0$. Clearly $(\alpha - 1) + (\beta - 1) = m - 2$ and $(\alpha - 1)(\beta - 1) = 1$. Recall that $\Delta = m^2 - 4m = (m-2)^2 - 4$. If $\Delta \neq 0$, then $\alpha \neq \beta$ and hence

$$\begin{aligned} u_n(m-2,1) =& \frac{(\alpha-1)^n - (\beta-1)^n}{(\alpha-1)-(\beta-1)} = \frac{(\alpha^2/m)^n - (\beta^2/m)^n}{\alpha - \beta} \\ =& \frac{\alpha^n - \beta^n}{\alpha - \beta} \cdot \frac{\alpha^n + \beta^n}{m^n} = \frac{u_n(m,m)v_n(m,m)}{m^n} \end{aligned}$$

for all $n \in \mathbb{N}$. In the case $\Delta = 0$ (i.e., $m = 4$), as

$$u_n(2,1) = n, \ u_n(4,4) = n2^{n-1} \text{ and } v_n(4,4) = 2^{n+1},$$

we also have

$$u_n(m-2,1) = n = \frac{n2^{n-1}2^{n+1}}{4^n} = \frac{u_n(m,m)v_n(m,m)}{m^n}.$$

So, for any $n \in \mathbb{N}$ we always have

$$u_n(m-2,1) = \frac{u_n(m,m)v_n(m,m)}{m^n}. \tag{2.10}$$

Note that $v_p(m,m) \equiv v_{p^0}(m,m) = m \pmod{p}$ by (2.4). In view of (2.10) and Lemma 2.3,

$$\begin{aligned} &2u_p(m,m) - u_p(m-2,1) \\ =& \frac{u_p(m,m)}{m^p}(m^p - v_p(m,m)) + u_p(m,m) \\ \equiv& \frac{(\frac{\Delta}{p})}{m}(m^p - v_p(m,m)) + u_p(m,m) \\ \equiv& \left(\frac{\Delta}{p}\right) m^{p-1} + u_p(m,m) - \left(\frac{\Delta}{p}\right)\frac{v_p(m,m)}{m} \pmod{p^2}. \end{aligned}$$

Thus, by the above, it suffices to prove the congruence

$$u_{p-(\frac{\Delta}{p})}(m,m)\frac{v_{p-(\frac{\Delta}{p})}(m,m)}{m^{p-(\frac{\Delta}{p})}}\equiv u_p(m,m)-\left(\frac{\Delta}{p}\right)\frac{v_p(m,m)}{m}\pmod{p^2}. \tag{2.11}$$

Clearly, $u_{p-(\frac{\Delta}{p})}(m,m)\equiv 0\pmod p$ by Lemma 2.3. If $p\mid\Delta$ then

$$v_{p-(\frac{\Delta}{p})}(m,m)=v_p(m,m)\equiv m\equiv m^p=m^{p-(\frac{\Delta}{p})}\pmod p$$

and hence (2.11) holds.

Now assume that $p\nmid\Delta$. Obviously,

$$\frac{v_{p-(\frac{\Delta}{p})}(m,m)}{m^{p-(\frac{\Delta}{p})}}\equiv\frac{2m^{(1-(\frac{\Delta}{p}))/2}}{m^{1-(\frac{\Delta}{p})}}=2m^{((\frac{\Delta}{p})-1)/2}\pmod p$$

by (2.7), and

$$u_{p-(\frac{\Delta}{p})}(m,m)=\frac{mu_p(m,m)-(\frac{\Delta}{p})v_p(m,m)}{2m^{(1+(\frac{\Delta}{p}))/2}}$$

by (2.8). Therefore the left-hand side of (2.11) is congruent to

$$\frac{mu_p(m,m)-(\frac{\Delta}{p})v_p(m,m)}{m}=u_p(m,m)-\left(\frac{\Delta}{p}\right)\frac{v_p(m,m)}{m}$$

modulo p^2. So (2.11) is valid and we are done. □

Proof of Theorem 1.1. Clearly (1.3) plus or minus (1.4) yields (1.5) or (1.6). Also, (1.4) follows from (1.3) by Lemma 2.1. So, it suffices to prove (1.3).

Combining Lemmas 2.2–2.4, we get

$$\begin{aligned}m^{p-1}\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^k}&\equiv 2u_{p^a}(m,m)-u_{p^a}(m-2,1)\\&\equiv\left(\frac{\Delta}{p^a}\right)m^{p-1}+u_{p^a-(\frac{\Delta}{p^a})}(m-2,1)\\&\equiv\left(\frac{\Delta}{p^{a-1}}\right)m^{p-1}\left(\left(\frac{\Delta}{p}\right)+u_{p-(\frac{\Delta}{p})}(m-2,1)\right)\pmod{p^2}.\end{aligned}$$

Therefore (1.3) holds. This concludes the proof. □

Proof of Corollary 1.1. By induction, $u_{2n}(0,1)=0$ and $u_n(2,1)=n$ for all $n\in\mathbb{N}$. Note also that

$$(-1)^{n-1}u_n(1,1)=u_n(-1,1)=\left(\frac{n}{3}\right)$$

and

$$(-1)^{n-1}u_n(-3,1)=u_n(3,1)=F_{2n}=F_nL_n,$$

where $L_n=v_n(1,-1)$. By [SS, Corollary 1] (or the proof of Corollary 1.3 of [ST1]), if $p\neq 2,5$ then $L_{p-(\frac{p}{5})}\equiv 2\left(\frac{p}{5}\right)\pmod{p^2}$.

In view of the above, we can easily deduce the congruences in Corollary 1.1 by applying Theorem 1.1. □

3. Proof of Theorem 1.2

Lemma 3.1. *Let p be an odd prime and let $k\in\mathbb{Z}$. Then*

$$\sum_{m=1}^{p-1}m^{pk}\equiv\begin{cases}p-1\pmod{p^2} & \text{if } p-1\mid k,\\ 0\pmod{p^2} & \text{otherwise.}\end{cases}$$

Proof. For $b,c\in\mathbb{Z}$ clearly $(b+cp)^p\equiv b^p\pmod{p^2}$. If $p-1\mid k$, then $m^{pk}\equiv 1\pmod{p^2}$ by Euler's theorem, and hence $\sum_{m=1}^{p-1}m^{pk}\equiv(p-1)\pmod{p^2}$.

Now suppose that $p-1\nmid k$ and let g be a primitive root modulo p. Then

$$g^{pk}\sum_{m=1}^{p-1}m^{pk}=\sum_{m=1}^{p-1}(gm)^{pk}\equiv\sum_{r=1}^{p-1}r^{pk}\pmod{p^2}$$

and hence

$$(g^{pk}-1)\sum_{m=1}^{p-1}m^{pk}\equiv 0\pmod{p^2}.$$

Since $g^{pk}-1$ is not divisible by p, we must have

$$\sum_{m=1}^{p-1}m^{pk}\equiv 0\pmod{p^2}.$$

This concludes the proof. □

Lemma 3.2. *Let p be an odd prime and let $a\in\mathbb{Z}^+$. Then, for any $r\in\mathbb{Z}$, we have*

$$\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2k}{k+1}\equiv\frac{1}{2}\sum_{\substack{0<k<p^a\\ k\equiv r+1\,(\mathrm{mod}\ p-1)}}\binom{2k}{k}-\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2k}{k}\pmod{p^2}$$

and

$$\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}C_k\equiv 2\sum_{\substack{0<k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2k}{k}-\frac{1}{2}\sum_{\substack{0<k<p^a\\ k\equiv r+1\,(\mathrm{mod}\ p-1)}}\binom{2k}{k}\pmod{p^2}.$$

Proof. For $k \in \mathbb{N}$ we have

$$\binom{2k}{k+1} + \binom{2k}{k} = \binom{2k+1}{k+1} = \frac{1}{2}\binom{2(k+1)}{k+1}.$$

Thus

$$\begin{aligned}&\sum_{\substack{0\leqslant k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2k}{k+1} + \sum_{\substack{0\leqslant k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2k}{k}\\ =&\frac{1}{2}\sum_{\substack{0\leqslant k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2(k+1)}{k+1} = \frac{1}{2}\sum_{\substack{1\leqslant k\leqslant p^a\\ k\equiv r+1\,(\mathrm{mod}\ p-1)}}\binom{2k}{k}\\ =&\frac{1}{2}\sum_{\substack{0<k<p^a\\ k\equiv r+1\,(\mathrm{mod}\ p-1)}}\binom{2k}{k} + R \pmod{p^2}\end{aligned}$$

where

$$R = \begin{cases} \frac{1}{2}\binom{2p^a}{p^a} = \binom{2p^a-1}{p^a-1} \equiv 1 \pmod{p^2} & \text{if } p-1 \mid r,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore the first congruence in Lemma 3.2 holds. This implies the second congruence in Lemma 3.2. We are done. □

Lemma 3.3. *Let $m, n \in \mathbb{N}$. Then*

$$\sum_{k=0}^{n}\binom{m}{k}(-4)^k\binom{2(n-k)}{n-k} = 4^n\prod_{k=1}^{n}\left(1-\frac{2m+1}{2k}\right).$$

Proof. For any $k \in \mathbb{N}$, clearly

$$\binom{2k}{k} = (-4)^k\binom{-1/2}{k}.$$

So we have

$$\begin{aligned}&\sum_{k=0}^{n}\binom{m}{k}(-4)^k\binom{2(n-k)}{n-k} = (-4)^n\sum_{k=0}^{n}\binom{m}{k}\binom{-1/2}{n-k}\\ =&(-4)^n\binom{m-1/2}{n} = (-2)^n\prod_{k=1}^{n}\frac{2m-2k+1}{k}.\end{aligned}$$

Therefore the desired congruence holds. □

Lemma 3.4. *Let p be an odd prime and let $r\in\{1,\ldots,(p-1)/2\}$. Then*

$$\begin{aligned}&\sum_{j=r}^{(p-1)/2}\binom{(p-1)/2}{j}(-4)^j\binom{2(p-1+r-j)}{p-1+r-j}\\&\quad\equiv -p\sum_{s=0}^{(p-1)/2-r}\frac{\binom{2r+2s}{r+s}}{(2s+1)\binom{2s}{s}}\pmod{p^2}.\end{aligned}$$

Proof. If $r\leqslant j\leqslant (p-1)/2$, then $0\leqslant j-r<(p-1)/2$. When $s\in\mathbb{N}$ and $s<(p-1)/2$, clearly

$$\begin{aligned}&\binom{2(p-1-s)}{p-1-s}=\prod_{0<t<p-s}\frac{p-1-s+t}{t}\\=&\frac{p}{s+1}\prod_{0<t\leqslant s}\frac{p+t-s-1}{t}\times\prod_{s+1<t<p-s}\frac{p+t-s-1}{t}\\\equiv&\frac{p}{s+1}(-1)^s\prod_{0<t\leqslant s}\frac{s-t+1}{t}\times\frac{(p-2(s+1))!}{(p-1-s)!/(s+1)!}\\\equiv&\frac{p}{s+1}(-1)^s\frac{(s+1)!}{\prod_{k=s+1}^{2s+1}(p-k)}\\\equiv&\frac{p(-1)^s s!}{(-1)^{s+1}\prod_{k=s+1}^{2s+1}k}=-\frac{p}{(2s+1)\binom{2s}{s}}\pmod{p^2}.\end{aligned}$$

Therefore

$$\begin{aligned}&\sum_{r\leqslant j\leqslant (p-1)/2}\binom{(p-1)/2}{j}(-4)^j\binom{2(p-1+r-j)}{p-1+r-j}\\\equiv&-p\sum_{r\leqslant j\leqslant (p-1)/2}\frac{\binom{-1/2}{j}(-4)^j}{(2(j-r)+1)\binom{2(j-r)}{j-r}}\\\equiv&-p\sum_{r\leqslant j\leqslant (p-1)/2}\frac{\binom{2j}{j}}{(2(r-j)+1)\binom{2(j-r)}{j-r}}\pmod{p^2}\end{aligned}$$

and hence the desired result follows. □

Lemma 3.5. *Let p be an odd prime and let $a\in\mathbb{Z}^+$ be even. Let m be an integer not divisible by p and set $\Delta=m(m-4)$. Then*

$$\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^k}\equiv\Delta^{(p-1)/2}\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^k}+\frac{\delta_m-\Delta^{p-1}}{2}\pmod{p^2},$$

where δ_m *takes* 0 *or* 1 *according as* $m \equiv 4 \pmod{p}$ *or not.*

Proof. By Theorem 1.1, $\sum_{k=0}^{p-1}\binom{2k}{k}/m^k \equiv (\frac{\Delta}{p}) \pmod{p}$ and

$$\begin{aligned}\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^k} \equiv & \left(\frac{\Delta}{p^{a-1}}\right)\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^k} = \left(\frac{\Delta}{p}\right)\left(\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^k}-\left(\frac{\Delta}{p}\right)\right)+\left(\frac{\Delta}{p}\right)^2\\ \equiv & \Delta^{(p-1)/2}\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^k}-\left(\frac{\Delta}{p}\right)\left(\Delta^{(p-1)/2}-\left(\frac{\Delta}{p}\right)\right) \pmod{p^2}.\end{aligned}$$

Since

$$\begin{aligned}\Delta^{p-1}-\delta_m = & \left(\Delta^{(p-1)/2}+\left(\frac{\Delta}{p}\right)\right)\left(\Delta^{(p-1)/2}-\left(\frac{\Delta}{p}\right)\right)\\ \equiv & 2\left(\frac{\Delta}{p}\right)\left(\Delta^{(p-1)/2}-\left(\frac{\Delta}{p}\right)\right) \pmod{p^2},\end{aligned}$$

the desired congruence follows from the above. □

Proof of Theorem 1.2. Let $d \in \{0,1\}$. In view of Lemma 3.1, we have

$$\begin{aligned}&(p-1)\sum_{\substack{0<k<p^a\\ k\equiv r \pmod{p-1}}}\binom{2k}{k+d}\\ \equiv & \sum_{k=1}^{p^a-1}\binom{2k}{k+d}\sum_{m=1}^{p-1}m^{p(r-k)} = \sum_{m=1}^{p-1}m^{pr}\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k+d}}{m^{pk}} \pmod{p^2}\end{aligned}$$

and hence

$$\sum_{\substack{0<k<p^a\\ k\equiv r \pmod{p-1}}}\binom{2k}{k+d} \bmod p^2$$

only depends on the parity of a by Theorem 1.1.

(i) If a is odd and $r \in \{1,\ldots,p-1\}$, then by the above we have

$$\sum_{\substack{0<k<p^a\\ k\equiv r \pmod{p-1}}}\binom{2k}{k+d} \equiv \sum_{\substack{0<k<p\\ k\equiv r \pmod{p-1}}}\binom{2k}{k+d} = \binom{2r}{r+d} \pmod{p^2}$$

for $d = 0,1$, therefore both (1.7) and (1.8) are valid.

(ii) Now we handle the case $2 \mid a$. By Lemma 3.2 it suffices to prove (1.9) for any given $r \in \{1,\ldots,p\}$.

In light of Lemmas 3.1 and 3.5,

$$\begin{aligned}
&(p-1)\sum_{\substack{0\leqslant k<p^a\\ k\equiv r\,(\mathrm{mod}\ p-1)}}\binom{2k}{k}\\
&\equiv\sum_{k=0}^{p^a-1}\binom{2k}{k}\sum_{m=1}^{p-1}m^{p(r-k)}=\sum_{m=1}^{p-1}m^{pr}\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^{pk}}\\
&\equiv\sum_{m=1}^{p-1}m^{pr}\left(m^p(m^p-4)\right)^{(p-1)/2}\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^{pk}}\\
&\quad+\sum_{m=1}^{p-1}m^{pr}\frac{\delta_m-(m^p(m^p-4))^{p-1}}{2}\pmod{p^2},
\end{aligned}$$

where δ_m is as in Lemma 3.5. (Note that $\delta_{m^p}=\delta_m$ since $m^p\equiv m\ (\mathrm{mod}\ p)$.)

Observe that

$$\begin{aligned}
&\sum_{m=1}^{p-1}m^{pr}(m^p(m^p-4))^{(p-1)/2}\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^{pk}}\\
=&\sum_{k=0}^{p-1}\binom{2k}{k}\sum_{m=1}^{p-1}m^{p((p-1)/2+r-k)}\sum_{j=0}^{(p-1)/2}\binom{(p-1)/2}{j}(-4)^jm^{p((p-1)/2-j)}\\
\equiv&\sum_{j=0}^{(p-1)/2}\binom{(p-1)/2}{j}(-4)^j\sum_{k=0}^{p-1}\binom{2k}{k}\sum_{m=1}^{p-1}m^{p(r-j-k)}\pmod{p^2}.
\end{aligned}$$

So, with the help of Lemma 3.1 we have

$$\begin{aligned}
&\frac{1}{p-1}\sum_{m=1}^{p-1}m^{pr}(m^p(m^p-4))^{(p-1)/2}\sum_{k=0}^{p-1}\frac{\binom{2k}{k}}{m^{pk}}\\
&\equiv\sum_{j=0}^{(p-1)/2}\binom{(p-1)/2}{j}(-4)^j\sum_{\substack{k=0\\ p-1\mid k+j-r}}^{p-1}\binom{2k}{k}\\
&\equiv\sum_{j=0}^{r}\binom{(p-1)/2}{j}(-4)^j\binom{2(r-j)}{r-j}\\
&\quad+\delta_{r,p-1}\binom{(p-1)/2}{0}(-4)^0+\delta_{r,p}\binom{(p-1)/2}{1}(-4)\\
&\quad+\delta_{r,p}\binom{(p-1)/2}{0}\left(\binom{2\times 1}{1}-\binom{2p}{p}\right)\\
&\quad+\sum_{r\leqslant j\leqslant(p-1)/2}\binom{(p-1)/2}{j}(-4)^j\binom{2(p-1+r-j)}{p-1+r-j}\pmod{p^2}.
\end{aligned}$$

Note that

$$\binom{2}{1}-\binom{2p}{p}\equiv 2-2\binom{2p-1}{p-1}\equiv 0 \pmod{p^2}.$$

By Lemma 3.3,

$$\sum_{j=0}^{r}\binom{(p-1)/2}{j}(-4)^r\binom{2(r-j)}{r-j}=4^r\prod_{0<k\leqslant r}\left(1-\frac{p}{2k}\right)$$

$$\equiv\begin{cases}4^r(1-pH_r/2) \pmod{p^2} & \text{if } 1\leqslant r<p-1,\\ 4^r \pmod{p^2} & \text{if } r=p-1,\\ 4^r(1-pH_{p-1}/2)/2\equiv 4^r/2 \pmod{p^2} & \text{if } r=p,\end{cases}$$

where H_r denotes the harmonic sum $\sum_{0<k\leqslant r}1/k$ and we note that

$$H_{p-1}=\frac{1}{2}\sum_{k=1}^{p-1}\left(\frac{1}{k}+\frac{1}{p-k}\right)=\frac{1}{2}\sum_{k=1}^{p-1}\frac{p}{k(p-k)}\equiv 0 \pmod{p}.$$

Combining the above and Lemma 3.4, we get

$$\frac{1}{p-1}\sum_{m=1}^{p-1}m^{pr}(m^p(m^p-4))^{(p-1)/2}\sum_{k=0}^{p-1}\frac{\binom{2k}{k+d}}{m^{pk}}$$

$$\equiv -pR_p(r)+\begin{cases}4^r(1-pH_r/2) \pmod{p^2} & \text{if } 1\leqslant r<p-1,\\ 4^r+1 \pmod{p^2} & \text{if } r=p-1,\\ 4^r/2-2p+2 \pmod{p^2} & \text{if } r=p.\end{cases}$$

Note also that

$$\frac{1}{p-1}\sum_{m=1}^{p-1}m^{pr}\left(\delta_m-(m^p(m^p-4))^{p-1}\right)$$

$$\equiv\frac{1}{p-1}\sum_{m=1}^{p-1}m^{pr}-\frac{4^{pr}}{p-1}-\sum_{k=0}^{p-1}\binom{p-1}{k}(-4)^k\frac{1}{p-1}\sum_{m=1}^{p-1}m^{p(p-1-k+r)}$$

$$\equiv\delta_{r,p-1}+(p+1)4^{pr}-\binom{p-1}{r}(-4)^r-\delta_{r,p}\binom{p-1}{1}(-4)-\delta_{r,p-1}\binom{p-1}{0}$$

$$\equiv 4^{pr}+p4^r+4(p-1)\delta_{r,p}-\begin{cases}4^r(1-pH_r) \pmod{p^2} & \text{if } 1\leqslant r<p-1,\\ 4^r \pmod{p^2} & \text{if } r=p-1,\\ 0 \pmod{p^2} & \text{if } r=p.\end{cases}$$

So, from the above, we finally obtain

$$\sum_{\substack{0\leqslant k<p^a\\ k\equiv r \pmod{p-1}}}\binom{2k}{k}\equiv\frac{(p+1)4^r+4^{pr}}{2}-pR_p(r)+\delta_{r,p-1} \pmod{p^2}.$$

Hence

$$\sum_{\substack{0<k<p^a\\ k\equiv r\ (\mathrm{mod}\ p-1)}}\binom{2k}{k}\equiv\frac{(p+1)4^r+4^{pr}}{2}-pR_p(r)\ (\mathrm{mod}\ p^2),$$

which is equivalent to (1.9) since

$$4^{pr}-4^r=4^r\left((1+(2^{p-1}-1))^{2r}-1\right)\equiv 4^r\times 2r(2^{p-1}-1)\ (\mathrm{mod}\ p^2).$$

So far we have completed the proof of Theorem 1.2. □

Proof of Corollary 1.2. Recall that $H_{p-1}\equiv 0\ (\mathrm{mod}\ p)$. As observed by Eisenstein,

$$\begin{aligned}\frac{2^p-2}{p}&=\sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}=\sum_{k=1}^{p-1}\frac{1}{k}\binom{p-1}{k-1}\\ \equiv&\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\equiv\sum_{k=1}^{p-1}\frac{(-1)^{k-1}-1}{k}=\sum_{j=1}^{(p-1)/2}\frac{-2}{2j}=-H_{(p-1)/2}\ (\mathrm{mod}\ p).\end{aligned}$$

It is easy to see that

$$\begin{aligned}C_{p-1}=&\frac{1}{p-1}\binom{2p-2}{p-2}=\frac{1}{2p-1}\prod_{k=1}^{p-1}\left(1+\frac{p}{k}\right)\\ &\equiv-(1+2p)(1+pH_{p-1})\equiv-1-2p\ (\mathrm{mod}\ p^2)\end{aligned}$$

and

$$\begin{aligned}C_{(p-1)/2}=&\frac{2}{p+1}\binom{p-1}{(p-1)/2}\\ =&\frac{2}{p+1}(-1)^{(p-1)/2}\prod_{k=1}^{(p-1)/2}\left(1-\frac{p}{k}\right)\\ \equiv&2(1-p)(-1)^{(p-1)/2}(1-pH_{(p-1)/2})\\ \equiv&2(-1)^{(p-1)/2}(1-p-pH_{(p-1)/2})\\ \equiv&2(-1)^{(p-1)/2}(2^p-p-1)\ (\mathrm{mod}\ p^2).\end{aligned}$$

So, by Theorem 1.2(i), (1.13)-(1.15) hold in the case $2\nmid a$.

From now on we assume that a is even.

Applying (1.12) with $r=p-1$ we immediately get (1.13). As

$$R_p\left(\frac{p-1}{2}\right)=\binom{p-1}{(p-1)/2}\equiv(-1)^{(p-1)/2}\ (\mathrm{mod}\ p)$$

and $R_p((p+1)/2)=0$, by (1.11) we have

$$\begin{aligned}\sum_{\substack{0<k<p^a\\ k\equiv(p-1)/2\,(\mathrm{mod}\ p-1)}} C_k \equiv& 4^{(p-1)/2}(2-2^p)-p2(-1)^{(p-1)/2}\\ \equiv& 2-2^p+(-1)^{(p+1)/2}2p \pmod{p^2}.\end{aligned}$$

This proves (1.15).

To obtain (1.14) we need to compute $R_p(1)$ and $R_p(2)$ modulo p. Observe that

$$\begin{aligned}R_p(1)=&\sum_{s=0}^{(p-1)/2-1}\frac{2\binom{2s+1}{s}}{(2s+1)\binom{2s}{s}}=\sum_{s=0}^{(p-3)/2}\frac{2}{s+1}\\ =&2H_{(p-1)/2}\equiv 2\times\frac{2-2^p}{p} \pmod{p}.\end{aligned}$$

When $p\geqslant 5$, we have

$$\begin{aligned}R_p(2)=&\sum_{s=0}^{(p-1)/2-2}\frac{2\binom{2s+3}{s+1}}{(2s+1)\binom{2s}{s}}=\sum_{s=0}^{(p-5)/2}\frac{4(2s+3)}{(s+1)(s+2)}\\ =&4\sum_{s=0}^{(p-5)/2}\left(\frac{1}{s+1}+\frac{1}{s+2}\right)=4(H_{(p-3)/2}+H_{(p-1)/2}-1)\\ =&8H_{(p-1)/2}-4\left(\frac{2}{p-1}+1\right)\equiv 8\times\frac{2-2^p}{p}+4 \pmod{p}.\end{aligned}$$

In the case $p=3$, as $R_3(2)=0$ we also have $R_p(2)\equiv 8(2-2^p)/p+4 \pmod{p}$. Applying (1.11) with $r=1$, we obtain

$$\begin{aligned}\sum_{\substack{0<k<p^a\\ k\equiv1\,(\mathrm{mod}\ p-1)}} C_k \equiv& 4(2-2^p)-p\left(2R_p(1)-\frac{R_p(2)}{2}\right)\\ \equiv& 4(2-2^p)-p(-2) \pmod{p^2}.\end{aligned}$$

So (1.14) follows.

The proof of Corollary 1.2 is now complete. □

REFERENCES

[CP] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd edition, Springer, New York, 2005.

[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, New York, 1994.

- [J] W. Jänichen, *Über die Verallgemeinerung einer Gauss'schen Formel aus der Theorie der höheren Kongruenzen*, Sitzungsber. Berl. Math. Ges. **20** (1921), 23–29.
- [PS] H. Pan and Z. W. Sun, *A combinatorial identity with application to Catalan numbers*, Discrete Math. **306** (2006), 1921–1940.
- [Sm] C. J. Smyth, *A coloring proof of a generalization of Fermat's little theorem*, Amer. Math. Monthly **93** (1986), 469–471.
- [St] R. P. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge Univ. Press, Cambridge, 1999.
- [SS] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371–388.
- [S92] Z. W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Ser. A **35** (1992), no.3, 257–269.
- [S02] Z. W. Sun, *On the sum $\sum_{k\equiv r\,(\mathrm{mod}\ m)}\binom{n}{k}$ and related congruences*, Israel J. Math. **128** (2002), 135–156.
- [S06] Z. W. Sun, *Binomial coefficients and quadratic fields*, Proc. Amer. Math. Soc. **134** (2006), 2213–2222.
- [S09] Z. W. Sun, *Various congruences involving binomial coefficients and higher-order Catalan numbers*, preprint, arXiv:0909.3808. `http://arxiv.org/abs/0909.3808`.
- [ST1] Z. W. Sun and R. Tauraso, *New congruences for central binomial coefficients*, Adv. in Math. **45** (2010), 125–148.
- [ST2] Z. W. Sun and R. Tauraso, *On some new congruences for binomial coefficients*, Int. J. Number Theory, in press. `http://arxiv.org/abs/0709.1665`.
- [V] E. B. Vinberg, *On some number-theoretic conjectures of V. Arnold*, Jpn. J. Math. **2** (2007), 297–302.
- [ZPS] L. L. Zhao, H. Pan and Z. W. Sun, *Some congruences for the second-order Catalan numbers*, Proc. Amer. Math. Soc. **138** (2010), 37–46.