Adv. in Appl. Math. 45(2010), no. 1, 125–148.

NEW CONGRUENCES FOR CENTRAL BINOMIAL COEFFICIENTS

Zhi-Wei Sun[1] and Roberto Tauraso[2]

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

[2]Dipartimento di Matematica
Università di Roma "Tor Vergata"
Roma 00133, Italy
tauraso@mat.uniroma2.it
http://www.mat.uniroma2.it/∼tauraso

Abstract. Let p be a prime and let a be a positive integer. In this paper we determine $\sum_{k=0}^{p^a-1}\binom{2k}{k+d}/m^k$ and $\sum_{k=1}^{p-1}\binom{2k}{k+d}/(km^{k-1})$ modulo p for all $d=0,\ldots,p^a$, where m is any integer not divisible by p. For example, we show that if $p\neq 2,5$ then

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

where F_n is the nth Fibonacci number and $(-)$ is the Jacobi symbol. We also prove that if $p>3$ then

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k}\equiv\frac{8}{9}p^2B_{p-3}\pmod{p^3},$$

where B_n denotes the nth Bernoulli number.

Key words and phrases. Central binomial coefficients, congruences modulo primes, Fibonacci numbers, Bernoulli numbers.

2010 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 05A19, 11A07, 11B39, 11B68.

The first author is the corresponding author, and he is supported by the National Natural Science Foundation (grant 10871087) and the Overseas Cooperation Fund (grant 10928101) of China.

1. Introduction

A central binomial coefficient has the form $\binom{2n}{n}$ with $n \in \mathbb{N} = \{0, 1, \ldots\}$. A well-known theorem of Wolstenholme (see, e.g., [5]) states that

$$\frac{1}{2}\binom{2p}{p} = \binom{2p-1}{p-1} \equiv 1 \pmod{p^3} \quad \text{for any prime } p > 3.$$

In 2006 H. Pan and Z. W. Sun [9] used a sophisticated combinatorial identity to deduce that if p is a prime then

$$\sum_{k=0}^{p-1}\binom{2k}{k+d} \equiv \left(\frac{p-d}{3}\right) \pmod{p} \quad \text{for } d = 0, \ldots, p, \tag{1.1}$$

where the Jacobi symbol $(\frac{a}{3})$ coincides with the unique integer $\varepsilon \in \{0, \pm 1\}$ satisfying $a \equiv \varepsilon \pmod 3$. In a recent paper [16] the authors determined $\sum_{k=0}^{p^a-1}\binom{2k}{k+d} \bmod p^2$ for any prime p and $d \in \{0, 1, \ldots, p^a\}$ with $a \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

In this paper we extend the congruence (1.1) in a new way and derive various congruences related to recurrences. Throughout this paper, for an assertion A we set

$$[A] = \begin{cases} 1 & \text{if } A \text{ holds,} \\ 0 & \text{otherwise.} \end{cases}$$

We also define two recurrences $\{u_n(x)\}_{n\in\mathbb{N}}$ and $\{v_n(x)\}_{n\in\mathbb{N}}$ of polynomials as follows:

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

and

$$v_0(x) = 2,\ v_1(x) = x,\ \text{and } v_{n+1}(x) = xv_n(x) - v_{n-1}(x)\ (n = 1, 2, \ldots).$$

For a fixed integer x, the sequences $\{u_n(x)\}_{n\in\mathbb{N}}$ and $\{v_n(x)\}_{n\in\mathbb{N}}$ are linear recurrences of integers. By induction, for any $n \in \mathbb{N}$ we have

$$u_n(-x) = (-1)^{n-1}u_n(x) \quad \text{and} \quad v_n(-x) = (-1)^n v_n(x). \tag{1.2}$$

Now we state our first theorem.

Theorem 1.1. *Let p be a prime and let $d \in \{0, \ldots, p^a\}$ with $a \in \mathbb{Z}^+$. Let $m \in \mathbb{Z}$ with $p \nmid m$. Then we have*

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

and

$$d\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k+d}}{km^{k-1}}\equiv 2(-1)^d+v_{p^a-d}(m-2)\pmod p\quad \text{provided } d>0. \tag{1.4}$$

If $p\neq 2$, then

$$\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k+d}}{m^k}\equiv -u_{d-(\frac{m(m-4)}{p^a})}(m-2)\pmod p \tag{1.5}$$

and also

$$d\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k+d}}{km^{k-1}}\equiv 2(-1)^d+v_{d-(\frac{m(m-4)}{p^a})}(m-2)\pmod p\ \text{provided } d>0, \tag{1.6}$$

where $u_{-1}(x)=xu_0(x)-u_1(x)=-1$ and $v_{-1}(x)=xv_0(x)-v_1(x)=x$.

Remark 1.1. Let p be any prime and let $a\in\mathbb{Z}^+$. As $u_n(-1)=(\frac{n}{3})$ for $n=0,1,2,\ldots$, (1.3) in the case $m=1$ yields that

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

Since $v_n(-1)=3[3\mid n]-1$ for all $n\in\mathbb{N}$, by (1.4) in the case $m=1$, for $d\in\{1,\ldots,p^a\}$ we have

$$d\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k+d}}{k}\equiv\begin{cases}2(-1)^d+2\pmod p & \text{if } p^a\equiv d\pmod 3,\\ 2(-1)^d-1\pmod p & \text{otherwise.}\end{cases}$$

The well-known Fibonacci sequence $\{F_n\}_{n\in\mathbb{N}}$ is defined by

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

Its companion $\{L_n\}_{n\in\mathbb{N}}$, the Lucas sequence, is given by

$$L_0=2,\ L_1=1,\ \text{and } L_{n+1}=L_n+L_{n-1}\ \text{for } n=1,2,3,\ldots.$$

Define

$$F_{-1}=F_1-F_0=1,\ F_{-2}=F_0-F_{-1}=-1,$$
$$L_{-1}=L_1-L_0=-1,\ L_{-2}=L_0-L_{-1}=3.$$

By induction, $F_{2n}=u_n(3)$ and $L_{2n}=v_n(3)$ for $n=-1,0,1,\ldots$. Note also that $u_{2n}(0)=v_{2n+1}(0)=0$ and $v_{2n}(0)/2=u_{2n+1}(0)=(-1)^n$ for all $n\in\mathbb{N}$. Thus, with the help of (1.2), Theorem 1.1 in the cases $m=-1,2$ gives the following consequence.

Corollary 1.1. *Let p be an odd prime and let $d \in \{0, 1, \ldots, p^a\}$ with $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1} (-1)^k \binom{2k}{k+d} \equiv (-1)^{d-[p\neq 5]} F_{2(d-(\frac{p^a}{5}))} \pmod{p}, \tag{1.7}$$

and

$$d \sum_{k=1}^{p^a-1} (-1)^k \frac{\binom{2k}{k+d}}{k} \equiv (-1)^{d-[p=5]} L_{2(d-(\frac{p^a}{5}))} - 2(-1)^d \pmod{p} \tag{1.8}$$

provided $d > 0$. Also,

$$\sum_{k=0}^{p^a-1} \frac{\binom{2k}{k+d}}{2^k} \equiv \begin{cases} 0 \pmod{p} & \text{if } p^a \equiv d \pmod{2}, \\ 1 \pmod{p} & \text{if } p^a \equiv d+1 \pmod{4}, \\ -1 \pmod{p} & \text{if } p^a \equiv d-1 \pmod{4}, \end{cases} \tag{1.9}$$

and for $d > 0$ we have

$$d \sum_{k=1}^{p^a-1} \frac{\binom{2k}{k+d}}{k2^k} - (-1)^d \equiv \begin{cases} 0 \pmod{p} & \text{if } p^a \not\equiv d \pmod{2}, \\ 1 \pmod{p} & \text{if } p^a \equiv d \pmod{4}, \\ -1 \pmod{p} & \text{if } p^a \equiv d+2 \pmod{4}. \end{cases} \tag{1.10}$$

Our following result can be viewed as a complement to Theorem 1.1.

Theorem 1.2. *Let p be a prime and let m be an integer not divisible by p. Then we have*

$$\frac{1}{2} \sum_{k=1}^{p-1} (-1)^k \frac{\binom{2k}{k}}{km^{k-1}} \equiv \frac{m^p - V_p(m)}{p} \pmod{p}, \tag{1.11}$$

where the polynomial sequence $\{V_n(x)\}_{n\in\mathbb{N}}$ is defined as follows:

$$V_0(x) = 2,\ V_1(x) = x,\ \text{and } V_{n+1}(x) = x(V_n(x) + V_{n-1}(x))\ (n \in \mathbb{Z}^+).$$

Given a prime p and an integer a not divisible by p, we use $q_p(a)$ to denote the integer $(a^{p-1} - 1)/p$ and call $q_p(a)$ a *Fermat quotient* with base a. See E. Lehmer [7] for connections between Fermat quotients and Fermat's last theorem.

Corollary 1.2. *Let p be an odd prime. Then*

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k2^{k-1}}\equiv\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k4^k}\equiv 2q_p(2)\ (\mathrm{mod}\ p). \tag{1.12}$$

If $p\neq 3$ then

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k3^{k-1}}\equiv 3q_p(3)\ (\mathrm{mod}\ p). \tag{1.13}$$

Corollary 1.3. *Let p be an odd prime.*

(i) *If $p\neq 5$, then we have*

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k}\equiv -5\frac{F_{p-(\frac{p}{5})}}{p}\ (\mathrm{mod}\ p), \tag{1.14}$$

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k5^k}\equiv q_p(5)-6\frac{F_{p-(\frac{p}{5})}}{p}\ (\mathrm{mod}\ p), \tag{1.15}$$

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k5^k}\equiv q_p(5)-\frac{F_{p-(\frac{p}{5})}}{p}\ (\mathrm{mod}\ p). \tag{1.16}$$

(ii) *Define the Pell sequence $\{P_n\}_{n\in\mathbb{N}}$ by*

$$P_0=0,\ P_1=1,\ \text{and}\ P_{n+1}=2P_n+P_{n-1}\ (n=1,2,3,\ldots).$$

Then

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k4^k}\equiv 2q_p(2)-4\frac{P_{p-(\frac{2}{p})}}{p}\equiv 2\sum_{0<k<3p/4}\frac{(-1)^{k-1}}{k}\ (\mathrm{mod}\ p). \tag{1.17}$$

(iii) *Let $\{S_n\}_{n\in\mathbb{N}}$ be the sequence defined by*

$$S_0=0,\ S_1=1,\ \text{and}\ S_{n+1}=4S_n-S_{n-1}\ (n=1,2,3,\ldots).$$

If $p>3$, then

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k2^k}\equiv q_p(2)-6\left(\frac{2}{p}\right)\frac{S_{(p-(\frac{3}{p}))/2}}{p}\equiv\sum_{0<k<5p/6}\frac{(-1)^{k-1}}{k}\ (\mathrm{mod}\ p) \tag{1.18}$$

and

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k6^k}\equiv q_p(2)+q_p(3)-2\left(\frac{2}{p}\right)\frac{S_{(p-(\frac{3}{p}))/2}}{p}\ (\mathrm{mod}\ p). \tag{1.19}$$

Remark 1.2. (a) A prime $p \neq 2,5$ is called a Wall-Sun-Sun prime if $F_{p-(\frac{p}{5})} \equiv 0 \pmod{p^2}$ (cf. [1]). In 1992 Z. H. Sun and Z. W. Sun [13] showed that Fermat's equation $x^p + y^p = z^p$ has no integer solutions satisfying $p \nmid xyz$ unless p is a Wall-Sun-Sun prime. There are no Wall-Sun-Sun primes below 2×10^{14} (cf. [8]). In 1982 H. C. Williams [10] showed that

$$\frac{F_{p-(\frac{p}{5})}}{p} \equiv \frac{2}{5} \sum_{0<k<4p/5} \frac{(-1)^k}{k} \pmod{p}.$$

(b) The second congruences in (1.17) and (1.18) are essentially due to Z. W. Sun [14, 15]. For other information about the sequence $\{S_n\}_{n\in\mathbb{N}}$ the reader may consult [11].

In 2006 Pan and Sun [9] proved that

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

for any prime $p > 3$. Here we determine the sum modulo p^3.

Theorem 1.3. *Let p be any prime and let $a \in \mathbb{Z}^+$. Then we have*

$$p^{a-1} \sum_{k=1}^{p^a-1} \frac{\binom{2k}{k}}{k} \equiv \begin{cases} 2 \pmod{p^3} & \text{if } p = 2, \\ 5 \pmod{p^3} & \text{if } p = 3, \\ \frac{8}{9}p^2 B_{p-3} \pmod{p^3} & \text{otherwise}, \end{cases} \tag{1.20}$$

where $B_0, B_1, B_2, \ldots$ are the well-known Bernoulli numbers.

The following conjecture, which is related to (1.7) in the case $d = 0$, seems very challenging.

Conjecture 1.1. *Let $p \neq 2,5$ be a prime and let $a \in \mathbb{Z}^+$. Then*

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

In the next section we are going to present two auxiliary identities. Theorem 1.1, Theorem 1.2 and Corollaries 1.2-1.3, and Theorem 1.3 will be proved in Sections 3, 4 and 5 respectively.

2. An auxiliary theorem

Theorem 2.1. *For any $n \in \mathbb{Z}^+$ and $d \in \mathbb{Z}$, we have*

$$\begin{aligned} &\sum_{0\leqslant k<n} \binom{2k}{k+d} x^{n-1-k} + [d>0]x^n u_d(x-2) \\ &= \sum_{0\leqslant k<n+d} \binom{2n}{k} u_{n+d-k}(x-2) \end{aligned} \tag{2.1}$$

and

$$\begin{aligned} &d\sum_{0<k<n}\frac{\binom{2k}{k+d}}{k}x^{n-k}-[d\geqslant 0]x^n v_d(x-2)+[d=0]x^n \\ &=-\sum_{0\leqslant k<n+d}\binom{2n}{k}v_{n+d-k}(x-2)-2\binom{2n-1}{n+d-1}. \end{aligned} \tag{2.2}$$

Proof. (i) We use induction on $n\in\mathbb{Z}^+$ to prove (2.1).

Since $(x-2)u_d(x-2)=u_{d+1}(x-2)+u_{d-1}(x-2)$ for $d=1,2,3,\ldots$, we can easily see that (2.1) with $n=1$ holds for all $d\in\mathbb{Z}$.

Now fix $n\in\mathbb{Z}^+$ and assume (2.1) for all $d\in\mathbb{Z}$. Let d be any integer. For $k\in\mathbb{N}$, it is easy to see that

$$\binom{2n+2}{k}=\binom{2n}{k}+2\binom{2n}{k-1}+\binom{2n}{k-2}.$$

Thus,

$$\begin{aligned} &\sum_{0\leqslant k<(n+1)+d}\binom{2n+2}{k}u_{n+1+d-k}(x-2) \\ =&\sum_{0\leqslant k<n+(d+1)}\binom{2n}{k}u_{n+(d+1)-k}(x-2) \\ &+2\sum_{0\leqslant j<n+d}\binom{2n}{j}u_{n+d-j}(x-2) \\ &+\sum_{0\leqslant i<n+(d-1)}\binom{2n}{i}u_{n+(d-1)-i}(x-2). \end{aligned}$$

By the induction hypothesis, for any $r\in\mathbb{Z}$ we have

$$\sum_{0\leqslant k<n+r}\binom{2n}{k}u_{n+r-k}(x-2)=\sum_{0\leqslant k<n}\binom{2k}{k+r}x^{n-1-k}+[r>0]x^n u_r(x-2).$$

So, from the above we get

$$\begin{aligned}
&\sum_{0\leqslant k<(n+1)+d}\binom{2n+2}{k}u_{n+1+d-k}(x-2)\\
=&\sum_{0\leqslant k<n}\left(\binom{2k}{k+d+1}+2\binom{2k}{k+d}+\binom{2k}{k+d-1}\right)x^{n-1-k}\\
&+[d\geqslant 0]x^n u_{d+1}(x-2)+2[d\geqslant 0]x^n u_d(x-2)+[d>0]x^n u_{d-1}(x-2)\\
=&\sum_{0\leqslant k<n}\left(\binom{2k+1}{k+d+1}+\binom{2k+1}{k+d}\right)x^{n-1-k}-[d=0]x^n u_{-1}(x-2)\\
&+[d\geqslant 0]x^n\left(u_{d+1}(x-2)+2u_d(x-2)+u_{d-1}(x-2)\right)\\
=&\sum_{0\leqslant k<n}\binom{2(k+1)}{(k+1)+d}x^{n-1-k}+[d=0]x^n+[d\geqslant 0]x^n x u_d(x-2)\\
=&\sum_{0\leqslant k<n+1}\binom{2k}{k+d}x^{(n+1)-1-k}+[d>0]x^{n+1}u_d(x-2).
\end{aligned}$$

This concludes the induction step and hence (2.1) holds.

(ii) By induction, $v_k(x-2)=2u_{k+1}(x-2)-(x-2)u_k(x-2)$ for all $k\in\mathbb{Z}$. Thus, with the help of (2.1), we have

$$\begin{aligned}
&\sum_{0\leqslant k\leqslant n+d}\binom{2n}{k}v_{n+d-k}(x-2)\\
=&2\sum_{0\leqslant k<n+d+1}\binom{2n}{k}u_{n+d+1-k}(x-2)\\
&-(x-2)\sum_{0\leqslant k<n+d}\binom{2n}{k}u_{n+d-k}(x-2)\\
=&2\sum_{0\leqslant k<n}\binom{2k}{k+d+1}x^{n-1-k}+[d+1>0]x^n 2u_{d+1}(x-2)\\
&-(x-2)\left(\sum_{0\leqslant k<n}\binom{2k}{k+d}x^{n-1-k}+[d>0]x^n u_d(x-2)\right)\\
=&\sum_{0\leqslant k<n}\left(2\binom{2k}{k+d+1}-(x-2)\binom{2k}{k+d}\right)x^{n-1-k}+[d\geqslant 0]x^n v_d(x-2).
\end{aligned}$$

For $k\in\mathbb{Z}^+$ we have

$$\begin{aligned}
&\binom{2k-2}{k+d}+\binom{2k-2}{k+d-1}=\binom{2k-1}{k+d}=\binom{2k-1}{k-d-1}\\
=&\frac{k-d}{2k}\binom{2k}{k-d}=\frac{k-d}{2k}\binom{2k}{k+d}=\frac{1}{2}\binom{2k}{k+d}-\frac{d}{2k}\binom{2k}{k+d}.
\end{aligned}$$

Thus

$$\begin{aligned}&\frac{1}{2}\sum_{0<k<n}\binom{2k}{k+d}x^{n-k}-\frac{d}{2}\sum_{0<k<n}\frac{\binom{2k}{k+d}}{k}x^{n-k}\\ =&\sum_{0<k\leqslant n}\left(\binom{2k-2}{k+d}+\binom{2k-2}{k+d-1}\right)x^{n-k}-\binom{(2n-2)+1}{n+d}\\ =&\sum_{0\leqslant k<n}\left(\binom{2k}{k+d+1}+\binom{2k}{k+d}\right)x^{n-1-k}-\binom{2n-1}{n+d}.\end{aligned}$$

It follows that

$$\begin{aligned}&d\sum_{0<k<n}\frac{\binom{2k}{k+d}}{k}x^{n-k}+[d=0]x^n-2\binom{2n-1}{n+d}\\ =&\sum_{0\leqslant k<n}\left((x-2)\binom{2k}{k+d}-2\binom{2k}{k+d+1}\right)x^{n-1-k}.\end{aligned}$$

Combining the above we obtain

$$\begin{aligned}&\sum_{0\leqslant k\leqslant n+d}\binom{2n}{k}v_{n+d-k}(x-2)-[d\geqslant 0]x^n v_d(x-2)\\ =&-d\sum_{0<k<n}\frac{\binom{2k}{k+d}}{k}x^{n-k}-[d=0]x^n+2\binom{2n-1}{n+d},\end{aligned}$$

from which (2.2) follows. □

Corollary 2.1. *Let $n\in\mathbb{Z}^+$ and $d\in\mathbb{N}$. Then*

$$\sum_{0\leqslant k<n}\binom{2k}{k+d}+\left(\frac{d}{3}\right)=\sum_{0\leqslant k<n+d}\binom{2n}{k}\left(\frac{n+d-k}{3}\right),\tag{2.3}$$

$$\sum_{0\leqslant k<n}(-1)^{k+d}\binom{2k}{k+d}+F_{2d}=\sum_{0\leqslant k<n+d}(-1)^k\binom{2n}{k}F_{2(n+d-k)},\tag{2.4}$$

and

$$\begin{aligned}&d\sum_{0<k<n}\frac{(-1)^{k+d}}{k}\binom{2k}{k+d}+\sum_{0\leqslant k<n+d}\binom{2n}{k}(-1)^kL_{2(n+d-k)}\\ &=L_{2d}-(-1)^{n+d}2\binom{2n-1}{n+d-1}-[d=0].\end{aligned}\tag{2.5}$$

Proof. For $j\in\mathbb{N}$ we have $u_j(-1)=\left(\frac{j}{3}\right)$, $(-1)^{j-1}u_j(-3)=u_j(3)=F_{2j}$ and $(-1)^jv_j(-3)=v_j(3)=L_{2j}$. Thus, (2.1) in the case $x=1$ yields (2.3), and (2.1) and (2.2) in the case $x=-1$ reduce to (2.4) and (2.5) respectively. This concludes the proof. □

3. Proof of Theorem 1.1

Given $A, B \in \mathbb{Z}$ we define the Lucas sequence $u_n = u_n(A,B)$ $(n \in \mathbb{N})$ and its companion $v_n = v_n(A,B)$ $(n \in \mathbb{N})$ as follows:

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

and

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

It is well known that

$$u_n = \sum_{0\leqslant k<n} \alpha^k\beta^{n-1-k} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for all } n \in \mathbb{N},$$

where α and β are the two roots of the equation $x^2 - Ax + B = 0$. It follows that if $n \in \mathbb{N}$ and $m \in \{n, n+1, \dots\}$ then

$$Au_n + v_n = 2u_{n+1} \quad \text{and} \quad u_m v_n - u_n v_m = 2B^n u_{m-n}.$$

Lemma 3.1. *Let $A, B \in \mathbb{Z}$ with $B \neq 0$. Let $u_n = u_n(A,B)$ for $n \in \mathbb{N}$, and define $u_{-1} = (u_1 - Au_0)/(-B) = -1/B$. Let p be an odd prime, and let $a \in \mathbb{Z}^+$ and $d \in \{0, 1, \dots, p^a\}$. Then we have*

$$B^d u_{p^a-d} \equiv -c(A,B)u_{d-(\frac{\Delta}{p^a})} \pmod p, \tag{3.1}$$

where $\Delta = A^2 - 4B$ and

$$c(A,B) = \begin{cases} A/2 & \text{if } p \mid \Delta, \\ B & \text{if } (\frac{\Delta}{p^a}) = 1, \\ 1 & \text{if } (\frac{\Delta}{p^a}) = -1. \end{cases}$$

Proof. The two roots of the equation $x^2 - Ax + B = 0$ are algebraic integers $\alpha = (A + \sqrt{\Delta})/2$ and $\beta = (A - \sqrt{\Delta})/2$. Since

$$\binom{p^a}{k} = \frac{p^a}{k}\binom{p^a-1}{k-1} \equiv 0 \pmod p \text{ for } k = 1, \dots, p^a - 1,$$

we have

$$v_{p^a} = \alpha^{p^a} + \beta^{p^a} \equiv (\alpha+\beta)^{p^a} = A^{p^a} \equiv A^{p^{a-1}} \equiv \cdots \equiv A \pmod p$$

with the help of Fermat's little theorem. If $\Delta \neq 0$, then

$$\begin{aligned} u_{p^a} =& \frac{\alpha^{p^a} - \beta^{p^a}}{\alpha - \beta} = \frac{1}{\sqrt{\Delta}} \left(\left(\frac{A+\sqrt{\Delta}}{2} \right)^{p^a} - \left(\frac{A-\sqrt{\Delta}}{2} \right)^{p^a} \right) \\ =& \frac{1}{2^{p^a}\sqrt{\Delta}} \sum_{\substack{k=0 \\ 2\nmid k}}^{p^a} \binom{p^a}{k} A^{p^a-k} \left((\sqrt{\Delta})^k - (-\sqrt{\Delta})^k \right) \\ =& \frac{1}{2^{p^a-1}} \sum_{\substack{k=1 \\ 2\nmid k}}^{p^a} \binom{p^a}{k} A^{p^a-k} \Delta^{(k-1)/2}; \end{aligned}$$

if $\Delta = 0$ then $\alpha = \beta = A/2$ and hence $u_{p^a} = p^a (A/2)^{p^a-1}$. So we always have

$$u_{p^a} = \frac{1}{2^{p^a-1}} \sum_{\substack{k=1 \\ 2\nmid k}}^{p^a} \binom{p^a}{k} A^{p^a-k} \Delta^{(k-1)/2}.$$

Note that $2^{p^a-1} \equiv 1 \pmod p$ by Fermat's little theorem. Thus, by Euler's criterion,

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

Observe that

$$2B^d u_{p^a-d} = u_{p^a} v_d - u_d v_{p^a} \equiv \left(\frac{\Delta}{p^a} \right) v_d - u_d A \pmod p.$$

When $p \mid \Delta$, this yields

$$B^d u_{p^a-d} \equiv -\frac{A}{2} u_d \pmod p.$$

If $(\frac{\Delta}{p^a}) = 1$, then

$$2B^d u_{p^a-d} \equiv v_d - A u_d = 2(u_{d+1} - A u_d) = -2B u_{d-1} \pmod p$$

and hence $B^d u_{p^a-d} \equiv -B u_{d-1} \pmod p$. If $(\frac{\Delta}{p^a}) = -1$, then

$$2B^d u_{p^a-d} \equiv -v_d - A u_d = -2u_{d+1} \pmod p$$

and thus $B^d u_{p^a-d} \equiv -u_{d+1} \pmod p$. So (3.1) follows. □

Proof of Theorem 1.1. For $n=-1,0,1,\ldots$ let $u_n=u_n(m-2)$ and $v_n=v_n(m-2)$.

By Theorem 2.1,

$$\sum_{k=0}^{p^a-1}\binom{2k}{k-d}m^{p^a-1-k}=\sum_{0\leqslant k<p^a-d}\binom{2p^a}{k}u_{p^a-d-k};$$

also, for $d>0$ we have

$$-d\sum_{0<k<p^a}\frac{\binom{2k}{k-d}}{k}m^{p^a-k}=-\sum_{0\leqslant k<p^a-d}\binom{2p^a}{k}v_{p^a-d-k}-2\binom{2p^a-1}{p^a-d-1}.$$

By Fermat's little theorem, $m^{p^a}\equiv m \pmod p$. For $k\in\{1,\ldots,p^a-1\}$ clearly

$$\binom{2p^a}{k}=\frac{2p^a}{k}\binom{2p^a-1}{k-1}\equiv 0 \pmod p;$$

also, if $d<p^a$ then

$$\binom{2p^a-1}{p^a-d-1}=\prod_{0<j<p^a-d}\left(\frac{2p^a}{j}-1\right)\equiv(-1)^{p^a-d-1}\equiv(-1)^d \pmod p.$$

Therefore

$$\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k+d}}{m^k}\equiv[d\neq p^a]\binom{2p^a}{0}u_{p^a-d}=u_{p^a-d} \pmod p;$$

if $d>0$ then

$$\begin{aligned}d\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k+d}}{km^{k-1}}\equiv&[d\neq p^a]\binom{2p^a}{0}v_{p^a-d}+2[d\neq p^a](-1)^d\\ \equiv&v_{p^a-d}+2(-1)^d \pmod p.\end{aligned}$$

So we have (1.3) and (1.4).

Now assume $p\neq 2$ and set $\Delta=(m-2)^2-4\times 1=m(m-4)$. As $p\nmid m$, if $p\mid\Delta$ then $m\equiv 4 \pmod p$ and hence $(m-2)/2\equiv 1 \pmod p$. Thus, with the help of Lemma 3.1, we have

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

which proves (1.5). If $d>0$, then

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

Thus (1.6) follows from (1.4). We are done. □

4. Proofs of Theorem 1.2 and Corollaries 1.2-1.3

Lemma 4.1. *For any positive integer n, we have*

$$\frac{1}{2}\sum_{0<k<n}\frac{\binom{2k}{k}}{kx^k}=\sum_{0<d<n}(-1)^{d-1}\sum_{0<k<n}\frac{\binom{2k}{k+d}}{kx^k}. \tag{4.1}$$

Proof. Observe that

$$\begin{aligned}&\sum_{d=0}^{n-1}(-1)^d\sum_{0<k<n}\frac{\binom{2k}{k+d}}{kx^k}\\
=&\sum_{0<k<n}\frac{1}{k(-x)^k}\sum_{d=0}^{n-1}(-1)^{k+d}\binom{2k}{k+d}\\
=&\sum_{0<k<n}\frac{1}{2k(-x)^k}\sum_{j=k}^{2k}\left((-1)^j\binom{2k}{j}+(-1)^{2k-j}\binom{2k}{2k-j}\right)\\
=&\sum_{0<k<n}\frac{1}{2k(-x)^k}\left((1-1)^{2k}+(-1)^k\binom{2k}{k}\right)=\frac{1}{2}\sum_{0<k<n}\frac{\binom{2k}{k}}{kx^k}.\end{aligned}$$

So (4.1) follows. □

Proof of Theorem 1.2. By Lemma 4.1,

$$\frac{1}{2}\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{km^{k-1}}=\sum_{d=1}^{p-1}(-1)^d\sum_{k=1}^{p-1}\frac{\binom{2k}{k+d}}{k(-m)^{k-1}}.$$

In view of (1.4) and the basic fact

$$\frac{1}{p}\binom{p}{d}=\frac{1}{d}\prod_{0<k<d}\frac{p-k}{k}\equiv\frac{(-1)^{d-1}}{d}\pmod p\quad(d=1,\ldots,p-1),$$

we have

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

Let α and β be the two roots of the equation $x^2-mx-m=0$. Then $(-\alpha-1)+(-\beta-1)=-m-2$ and $(-\alpha-1)(-\beta-1)=1$, also

$$V_p(m)=\alpha^p+\beta^p\equiv(\alpha+\beta)^p=m^p\equiv m \pmod p.$$

In the case $p\neq 2$, we have

$$\begin{aligned}&\sum_{k=1}^{p-1}\binom{p}{k}v_k(-m-2)=\sum_{k=1}^{p-1}\binom{p}{k}((-\alpha-1)^k+(-\beta-1)^k)\\ =&(-\alpha)^p+(-\beta)^p-2-(-\alpha-1)^p-(-\beta-1)^p\\ =&(-1)^pV_p(m)-2-(-1)^p\frac{\alpha^{2p}+\beta^{2p}}{m^p}\\ =&-V_p(m)+\frac{(\alpha^p+\beta^p)^2}{m^p}=\left(1+\frac{V_p(m)-m^p}{m^p}\right)(V_p(m)-m^p)\\ \equiv&V_p(m)-m^p \pmod{p^2}\quad(\text{since } V_p(m)\equiv m^p \pmod p).\end{aligned}$$

Note also that

$$\sum_{k=1}^{2-1}\binom{2}{k}v_k(-m-2)=2(-m-2)\equiv 2m=V_2(m)-m^2 \pmod{2^2}.$$

Therefore (1.11) follows from the above. □

Proof of Corollary 1.2. By induction, whenever $n\in\mathbb{N}$ we have

$$\begin{aligned}&V_{4n}(-2)=(-1)^n2^{2n+1},\ V_{4n+1}(-2)=(-1)^{n+1}2^{2n+1},\\ &V_{4n+2}(-2)=0,\ V_{4n+3}(-2)=(-1)^n2^{2n+2}.\end{aligned}$$

It follows that

$$V_p(-2)=-\left(\frac{2}{p}\right)2^{(p+1)/2}.$$

Combining this with (1.11) in the case $m=-2$, we get

$$\begin{aligned}\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k2^k}\equiv&\frac{V_p(-2)-(-2)^p}{p}=2^{(p+1)/2}\frac{2^{(p-1)/2}-(\frac{2}{p})}{p}\\ \equiv&\left(2^{(p-1)/2}+\left(\frac{2}{p}\right)\right)\frac{2^{(p-1)/2}-(\frac{2}{p})}{p}=q_p(2) \pmod p.\end{aligned}$$

By induction, $V_n(-4)=(-1)^n2^{n+1}$ for all $n\in\mathbb{N}$. Thus, by (1.11) with $m=-4$, we have

$$\frac{1}{2}\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k4^{k-1}}\equiv\frac{V_p(-4)-(-4)^p}{p}=2^p\frac{2^p-2}{p}\equiv 4q_p(2) \pmod p.$$

Therefore (1.12) holds.

Now assume that $p \neq 3$. By induction, for $n \in \mathbb{N}$ we have

$$V_n(-3) = \begin{cases} (3[3 \mid n] - 1)(-3)^{n/2} & \text{if } 2 \mid n, \\ (\frac{n}{3})(-3)^{(n+1)/2} & \text{if } 2 \nmid n. \end{cases}$$

Applying (1.11) with $m = -3$ we get

$$\begin{aligned} \frac{1}{2}\sum_{k=1}^{p-1} \frac{\binom{2k}{k}}{k3^{k-1}} \equiv & \frac{V_p(-3) - (-3)^p}{p} = -(-3)^{(p+1)/2} \frac{(-3)^{(p-1)/2} - (\frac{-3}{p})}{p} \\ \equiv & \frac{3}{2}\left((-3)^{(p-1)/2} + \left(\frac{-3}{p}\right)\right)\frac{(-3)^{(p-1)/2} - (\frac{-3}{p})}{p} \\ \equiv & \frac{3}{2} \cdot \frac{(-3)^{p-1} - 1}{p} = \frac{3}{2} q_p(3) \pmod{p}. \end{aligned}$$

So (1.13) is valid. $\square$

Proof of Corollary 1.3. (i) Applying Theorem 1.2 with $m = 1$, we obtain that

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

Let α and β be the two roots of the equation $x^2 - x - 1 = 0$. Suppose $p \neq 5$ and set $n = (p - (\frac{p}{5}))/2$. It is known that

$$L_n^2 - 5F_n^2 = (\alpha^n + \beta^n)^2 - (\alpha - \beta)^2 \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 = 4(\alpha\beta)^n = 4(-1)^n$$

and

$$L_{2n} = \alpha^{2n} + \beta^{2n} = (\alpha^n + \beta^n)^2 - 2(\alpha\beta)^n = L_n^2 - 2(-1)^n.$$

By [13, Corollary 1], $p \mid F_n$ if $p \equiv 1 \pmod 4$, and $p \mid L_n$ if $p \equiv 3 \pmod 4$. Thus

$$L_{p-(\frac{p}{5})} = L_{2n} = 5F_n^2 + 2(-1)^n = L_n^2 - 2(-1)^n \equiv 2\left(\frac{p}{5}\right) \pmod{p^2}.$$

By induction,

$$2L_k = 5F_{k-1} + L_{k-1} = 5F_{k+1} - L_{k+1} \text{ for } k = 1, 2, 3, \ldots .$$

Therefore

$$2L_p = 5F_{p-(\frac{p}{5})} + \left(\frac{p}{5}\right) L_{p-(\frac{p}{5})} \equiv 5F_{p-(\frac{p}{5})} + 2 \pmod{p^2}$$

and hence

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k}\equiv -2\frac{L_p-1}{p}\equiv -5\frac{F_{p-(\frac{p}{5})}}{p} \pmod p.$$

This proves (1.14).

By (1.11) in the case $m=5$,

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k5^k}\equiv \frac{2}{5}\cdot\frac{5^p-V_p(5)}{p} \pmod p.$$

Since $(5+3\sqrt{5})/2$ and $(5-3\sqrt{5})/2$ are the two roots of the equation $x^2-5x-5=0$,

$$\begin{aligned}V_p(5)=&\left(\frac{5+3\sqrt{5}}{2}\right)^p+\left(\frac{5-3\sqrt{5}}{2}\right)^p\\ =&\sqrt{5}^p\left(\left(\frac{1+\sqrt{5}}{2}\right)^{2p}-\left(\frac{1-\sqrt{5}}{2}\right)^{2p}\right)\\ =&5^{(p+1)/2}\frac{\alpha^p-\beta^p}{\alpha-\beta}(\alpha^p+\beta^p)=5^{(p+1)/2}F_pL_p.\end{aligned}$$

As

$$L_p\equiv 1+\frac{5}{2}F_{p-(\frac{5}{p})} \pmod{p^2}$$

and

$$L_p=F_p+2F_{p-1}=2F_{p+1}-F_p=2F_{p-(\frac{p}{5})}+\left(\frac{p}{5}\right)F_p,$$

we have

$$\begin{aligned}&\left(\frac{p}{5}\right)F_pL_p=L_p(L_p-2F_{p-(\frac{p}{5})})\\ \equiv&\left(1+\frac{5}{2}F_{p-(\frac{p}{5})}\right)\left(1+\frac{1}{2}F_{p-(\frac{p}{5})}\right)\equiv 1+3F_{p-(\frac{p}{5})} \pmod{p^2}\end{aligned}$$

and hence

$$\begin{aligned}&V_p(5)=5^{(p+1)/2}F_pL_p\\ \equiv&5^{(p+1)/2}\left(\frac{5}{p}\right)(1+3F_{p-(\frac{p}{5})})\equiv 5^{(p+1)/2}\left(\frac{5}{p}\right)+15F_{p-(\frac{p}{5})} \pmod{p^2}.\end{aligned}$$

Therefore

$$\begin{aligned}\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k5^k} \equiv&\frac{2}{5}\cdot\frac{5^p-5^{(p+1)/2}(\frac{5}{p})-15F_{p-(\frac{p}{5})}}{p}\\ \equiv&\left(5^{(p-1)/2}+\left(\frac{5}{p}\right)\right)\frac{5^{(p-1)/2}-(\frac{5}{p})}{p}-6\frac{F_{p-(\frac{p}{5})}}{p}\\ \equiv&q_p(5)-6\frac{F_{p-(\frac{p}{5})}}{p} \pmod p.\end{aligned}$$

So (1.15) also holds.

Applying (1.11) with $m=-5$ we get

$$\frac{1}{2}\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k5^{k-1}}\equiv\frac{V_p(-5)+5^p}{p} \pmod p.$$

As the two roots of the equation $x^2+5x+5=0$ are $(-5\pm\sqrt{5})/2$, we have

$$\begin{aligned}V_p(-5)=&\left(\frac{-5+\sqrt{5}}{2}\right)^p+\left(\frac{-5-\sqrt{5}}{2}\right)^p\\ =&\sqrt{5}^p\left(\left(\frac{1-\sqrt{5}}{2}\right)^p-\left(\frac{1+\sqrt{5}}{2}\right)^p\right)=-\sqrt{5}^{p+1}F_p.\end{aligned}$$

Recall that

$$\left(\frac{5}{p}\right)F_p=L_p-2F_{p-(\frac{p}{5})}\equiv 1+\frac{1}{2}F_{p-(\frac{p}{5})} \pmod{p^2}.$$

Thus

$$\begin{aligned}5^{(p-1)/2}F_p-1\equiv&5^{(p-1)/2}\left(\frac{5}{p}\right)\left(1+\frac{1}{2}F_{p-(\frac{p}{5})}\right)-1\\ \equiv&\left(\frac{5}{p}\right)\left(5^{(p-1)/2}-\left(\frac{5}{p}\right)\right)+\frac{1}{2}F_{p-(\frac{p}{5})}\\ \equiv&\frac{1}{2}\left(5^{(p-1)/2}+\left(\frac{5}{p}\right)\right)\left(5^{(p-1)/2}-\left(\frac{5}{p}\right)\right)+\frac{1}{2}F_{p-(\frac{p}{5})}\\ \equiv&\frac{5^{p-1}-1}{2}+\frac{1}{2}F_{p-(\frac{p}{5})} \pmod{p^2}\end{aligned}$$

and hence

$$\begin{aligned}\frac{1}{2}\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k5^{k-1}}\equiv&\frac{5^p-5^{(p+1)/2}F_p}{p}=\frac{5^p-5}{p}-5\frac{5^{(p-1)/2}F_p-1}{p}\\ \equiv&5\left(q_p(5)-\frac{q_p(5)}{2}-\frac{F_{p-(\frac{p}{5})}}{2p}\right) \pmod p.\end{aligned}$$

This proves (1.16).

(ii) As $2+2\sqrt{2}$ and $2-2\sqrt{2}$ are the two roots of the equation $x^2-4x-4=0$, we have

$$V_p(4)=(2+2\sqrt{2})^p+(2-2\sqrt{2})^p=2^p\left((1+\sqrt{2})^p+(1-\sqrt{2})^p\right)=2^pQ_p,$$

where the sequence $\{Q_n\}_{n\in\mathbb{N}}$ is given by

$$Q_0=Q_1=2 \text{ and } Q_{n+1}=2Q_n+Q_{n-1}\ (n=1,2,3,\ldots).$$

By [15, Remark 3.1],

$$4\left(\frac{2}{p}\right)P_p-Q_p=\left(\frac{2}{p}\right)Q_{p-(\frac{2}{p})}\equiv 2 \pmod{p^2}$$

and

$$P_{p-(\frac{2}{p})}\equiv\left(\frac{2}{p}\right)P_p-1 \pmod{p^2}.$$

Thus

$$Q_p-2\equiv 4\left(\left(\frac{2}{p}\right)P_p-1\right)\equiv 4P_{p-(\frac{2}{p})} \pmod{p^2}$$

and hence

$$\begin{aligned}\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k4^k}\equiv&\frac{4^p-V_p(4)}{2p}=2^{p-1}\frac{2^p-Q_p}{p}\\ \equiv&2q_p(2)-\frac{Q_p-2}{p}\equiv 2q_p(2)-4\frac{P_{p-(\frac{2}{p})}}{p} \pmod{p}\end{aligned}$$

with the help of (1.11) in the case $m=4$.

By [14],

$$-2^{(p+1)/2}\frac{P_p-2^{(p-1)/2}}{p}\equiv\sum_{k=1}^{(p-1)/2}\frac{1}{k2^k}\equiv\sum_{k=1}^{\lfloor 3p/4\rfloor}\frac{(-1)^{k-1}}{k} \pmod{p}.$$

(The last congruence was first conjectured by Z. H. Sun in 1988.) Observe that

$$\begin{aligned}-2^{(p+1)/2}\frac{P_p-2^{(p-1)/2}}{p}\equiv&-2^{(p+1)/2}\frac{(\frac{2}{p})(1+P_{p-(\frac{2}{p})})-2^{(p-1)/2}}{p}\\ \equiv&-2\frac{P_{p-(\frac{2}{p})}}{p}+2^{(p+1)/2}\frac{2^{(p-1)/2}-(\frac{2}{p})}{p}\\ \equiv&-2\frac{P_{p-(\frac{2}{p})}}{p}+q_p(2) \pmod{p}.\end{aligned}$$

So we also have

$$2q_p(2) - 4\frac{P_{p-(\frac{2}{p})}}{p} \equiv 2\sum_{k=1}^{\lfloor 3p/4\rfloor}\frac{(-1)^{k-1}}{k} \pmod{p}.$$

(iii) Now suppose $p > 3$. By Theorem 1.2 in the case $m = 2$, we have

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k2^k} \equiv \frac{2^p - V_p(2)}{p} \pmod{p}.$$

Observe that the two roots of the equation $x^2 - 2x - 2 = 0$ are $1 \pm \sqrt{3}$. Thus

$$\begin{aligned}V_p(2) =&(1+\sqrt{3})^p + (1-\sqrt{3})^p = 2\sum_{k=0}^{(p-1)/2}\binom{p}{2k}(\sqrt{3})^{2k}\\ =&2 + \sum_{k=1}^{(p-1)/2}\frac{2p}{2k}\binom{p-1}{2k-1}3^k\\ \equiv&2 - p\sum_{k=1}^{(p-1)/2}\frac{3^k}{k} \pmod{p^2}.\end{aligned}$$

As observed by Eisenstein [2],

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

By a congruence of Z. W. Sun [15],

$$\sum_{k=1}^{(p-1)/2}\frac{3^k}{k} \equiv \sum_{0<k<p/6}\frac{(-1)^k}{k} \equiv \sum_{0<k<p/6}\frac{(-1)^{p-k}}{p-k} \pmod{p}.$$

Thus

$$\begin{aligned}&\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k2^k}\\ \equiv&\frac{2^p-2}{p} - \frac{V_p(2)-2}{p} \equiv 2q_p(2) + \sum_{k=1}^{(p-1)/2}\frac{3^k}{k}\\ \equiv&\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k} + \sum_{5p/6<k<p}\frac{(-1)^k}{k} = \sum_{0<k<5p/6}\frac{(-1)^{k-1}}{k} \pmod{p}.\end{aligned}$$

In light of [15],

$$\sum_{k=1}^{(p-1)/2}\frac{3^k}{k}\equiv -q_p(2)-6\left(\frac{2}{p}\right)\frac{S_{(p-(\frac{3}{p}))/2}}{p}\pmod p.$$

So we also have

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k2^k}\equiv q_p(2)-6\left(\frac{2}{p}\right)\frac{S_{(p-(\frac{3}{p}))/2}}{p}\pmod p.$$

Therefore (1.18) follows.

Let $u_n=u_n(2,-2)$ and $v_n=v_n(2,-2)$ for $n\in\mathbb{N}$. By induction,

$$v_n=2u_{n+1}-2u_n=2u_n+4u_{n-1}\quad\text{for } n=1,2,3,\ldots.$$

Thus

$$v_p=2\left(\frac{3}{p}\right)u_p+\left(3+\left(\frac{3}{p}\right)\right)u_{p-(\frac{3}{p})}.$$

Clearly

$$\begin{aligned}2\sqrt{3}u_{p-(\frac{3}{p})}=&(1+\sqrt{3})^{p-(\frac{3}{p})}-(1-\sqrt{3})^{p-(\frac{3}{p})}\\=&2^{(p-(\frac{3}{p}))/2}\left((2+\sqrt{3})^{(p-(\frac{3}{p}))/2}-(2-\sqrt{3})^{(p-(\frac{3}{p}))/2}\right)\end{aligned}$$

and hence

$$u_{p-(\frac{3}{p})}=2^{(p-(\frac{3}{p}))/2}S_{(p-(\frac{3}{p}))/2}\equiv\left(\frac{2}{p}\right)2^{(1-(\frac{3}{p}))/2}S_{(p-(\frac{3}{p}))/2}\pmod{p^2}.$$

Recall that

$$v_p=V_p(2)\equiv 2-p\sum_{k=1}^{(p-1)/2}\frac{3^k}{k}\equiv 2+(2^{p-1}-1)+6\left(\frac{2}{p}\right)S_{(p-(\frac{3}{p}))/2}\pmod{p^2}.$$

Therefore

$$\begin{aligned}&2\left(\frac{3}{p}\right)u_p-2=v_p-2-\left(3+\left(\frac{3}{p}\right)\right)u_{p-(\frac{3}{p})}\\\equiv&2^{p-1}-1+6\left(\frac{2}{p}\right)S_{(p-(\frac{3}{p}))/2}-\left(3+\left(\frac{3}{p}\right)\right)\left(\frac{2}{p}\right)2^{(1-(\frac{3}{p}))/2}S_{(p-(\frac{3}{p}))/2}\\\equiv&2^{p-1}-1+2\left(\frac{2}{p}\right)S_{(p-(\frac{3}{p}))/2}\pmod{p^2}.\end{aligned}$$

Applying (1.11) with $m=-6$, we get

$$\frac{1}{2}\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k6^{k-1}}\equiv\frac{V_p(-6)+6^p}{p}\equiv\frac{V_p(-6)+6}{p}+6(q_p(2)+q_p(3)) \pmod p.$$

Observe that

$$\begin{aligned}V_p(-6)=&(-3+\sqrt{3})^p+(-3-\sqrt{3})^p\\ =&-\sqrt{3}^p\left((1+\sqrt{3})^p-(1-\sqrt{3})^p\right)=-2\times 3^{(p+1)/2}u_p\end{aligned}$$

and hence

$$\begin{aligned}V_p(-6)+6\equiv&-6\left(3^{(p-1)/2}-\left(\frac{3}{p}\right)\right)u_p-6\left(\frac{3}{p}\right)u_p+6\\ \equiv&-6\left(3^{(p-1)/2}-\left(\frac{3}{p}\right)\right)\left(\frac{3}{p}\right)\\ &-3\left(2^{p-1}-1+2\left(\frac{2}{p}\right)S_{(p-(\frac{3}{p}))/2}\right)\\ \equiv&-3\left((3^{p-1}-1)+2^{p-1}-1+2\left(\frac{2}{p}\right)S_{(p-(\frac{3}{p}))/2}\right) \pmod{p^2}.\end{aligned}$$

Therefore

$$\begin{aligned}\frac{1}{2}\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k6^{k-1}}\equiv&-3\Bigg(q_p(3)+q_p(2)+2\left(\frac{2}{p}\right)\frac{S_{(p-(\frac{3}{p}))/2}}{p}\Bigg)\\ &+6(q_p(2)+q_p(3))\\ \equiv&3\Bigg(q_p(2)+q_p(3)-2\left(\frac{2}{p}\right)\frac{S_{(p-(\frac{3}{p}))/2}}{p}\Bigg) \pmod p.\end{aligned}$$

So (1.19) is valid.

The proof of Corollary 1.3 is now complete. □

5. Proof of Theorem 1.3

Proof of Theorem 1.3. By an identity of T. B. Staver [12],

$$\sum_{k=1}^{n}\frac{1}{k}\binom{2k}{k}=\frac{2n+1}{3n^2}\binom{2n}{n}\sum_{k=1}^{n}\frac{1}{\binom{n-1}{k-1}^2}=\frac{n+1}{3}\binom{2n+1}{n}\sum_{k=1}^{n}\frac{1}{k^2\binom{n}{k}^2}$$

for all $n=1,2,3,\ldots$. Taking $n=p^a-1$ in the identity, we get

$$\sum_{k=1}^{p^a-1}\frac{1}{k}\binom{2k}{k}=\frac{p^a}{3}\binom{2p^a-1}{p^a-1}\sum_{k=1}^{p^a-1}\frac{1}{k^2\binom{p^a-1}{k}^2}. \tag{5.1}$$

Recall that

$$\binom{2p^a-1}{p^a-1} \equiv 1 + p[p=2] + p^2[p=3] \pmod{p^3}$$

by [16, Lemma 2.2]. For $k = 1, \ldots, p^a - 1$, we set $H_k = \sum_{0<j\leqslant k} 1/j$ and note that

$$\begin{aligned}\frac{1}{\binom{p^a-1}{k}^2} &= \prod_{0<j\leqslant k} \frac{1}{(1-p^a/j)^2} \\ &\equiv \prod_{0<j\leqslant k} \frac{(1-p^{3a}/j^3)^2}{(1-p^a/j)^2} = \prod_{0<j\leqslant k}\left(1+\frac{p^a}{j}+\frac{p^{2a}}{j^2}\right)^2 \\ &\equiv \prod_{0<j\leqslant k}\left(1+2\frac{p^a}{j}+\frac{p^{2a}}{j^2}+2\frac{p^{2a}}{j^2}\right) \pmod{p^3} \\ &\equiv \prod_{0<j\leqslant k}\left(1+2\frac{p^a}{j}\right) \pmod{p^{2+[p=3]}}\end{aligned}$$

Therefore (5.1) implies that

$$\begin{aligned} p^{a-1}\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k}}{k} &= \frac{p}{3}\binom{2p^a-1}{p^a-1}\sum_{k=1}^{p^a-1}\frac{p^{2(a-1)}}{k^2\binom{p^a-1}{k}^2} \\ \equiv& \frac{p}{3}(1+p[p=2]+p^2[p=3])\sum_{k=1}^{p^a-1}\frac{p^{2(a-1)}}{k^2}\prod_{0<j\leqslant k}\left(1+2\frac{p^a}{j}\right) \pmod{p^3}.\end{aligned}$$

So we have

$$p^{a-1}\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k}}{k} \equiv \left(\frac{p}{3}+p^2[p\leqslant 3]\right)\sum_{k=1}^{p^a-1}\frac{p^{2(a-1)}}{k^2}\prod_{0<j\leqslant k}\left(1+2\frac{p^a}{j}\right) \pmod{p^3}. \tag{5.2}$$

For $k = 1, \ldots, p^a - 1$, clearly

$$\begin{aligned}\prod_{0<j\leqslant k}\left(1+2\frac{p^a}{j}\right) \equiv& 1+2p^aH_k+4p^{2a}\sum_{0<i<j\leqslant k}\frac{1}{ij} \\ \equiv& 1+2p^aH_k+2p^{2a}\left(H_k^2-\sum_{j=1}^{k}\frac{1}{j^2}\right) \pmod{p^3}.\end{aligned}$$

In the case $a \geqslant 2$, if $1 \leqslant k \leqslant p^a - 1$ and $p^{a-2} \nmid k$ then $p^{2(a-1)}/k^2 \equiv$

$0 \pmod{p^4}$. When $a \geqslant 2$ and $k \in \{1, \dots, p^2-1\}$, we have

$$\begin{aligned}\prod_{j=1}^{p^{a-2}k}\left(1+2\frac{p^a}{j}\right) \equiv& 1+2\sum_{j=1}^{p^{a-2}k}\frac{p^a}{j}+2\bigg(\sum_{j=1}^{p^{a-2}k}\frac{p^a}{j}\bigg)^2-2\sum_{j=1}^{p^{a-2}k}\frac{p^{2a}}{j^2}\\ \equiv& 1+2\sum_{i=1}^{k}\frac{p^a}{p^{a-2}i}+2\bigg(\sum_{i=1}^{k}\frac{p^a}{p^{a-2}i}\bigg)^2-2\sum_{i=1}^{k}\frac{p^{2a}}{(p^{a-2}i)^2}\\ \equiv& 1+2p^2H_k+2(p^2H_k)^2-2\sum_{i=1}^{k}\frac{p^4}{i^2} \pmod{p^3}.\end{aligned}$$

Therefore, if $a \geqslant 2$ then (5.2) implies that

$$\begin{aligned}p^{a-1}\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k}}{k} &\equiv \left(\frac{p}{3}+p^2[p\leqslant 3]\right)\sum_{k=1}^{p^2-1}\frac{p^{2(a-1)}}{(p^{a-2}k)^2}\prod_{j=1}^{p^{a-2}k}\left(1+2\frac{p^a}{j}\right)\\ &\equiv \left(\frac{p}{3}+p^2[p\leqslant 3]\right)\sum_{k=1}^{p^2-1}\frac{p^2}{k^2}\prod_{j=1}^{k}\left(1+2\frac{p^2}{j}\right) \pmod{p^3}.\end{aligned}$$

In the case $p=3$, this yields (1.20) for $a \geqslant 2$. (1.20) in the case $p=3$ and $a=1$ can be verified directly.

Below we assume that $p \neq 3$. For $k=1,\dots,p^a-1$, if $p^{a-1} \nmid k$ then $p^{2(a-1)}/k^2 \equiv 0 \pmod{p^2}$. Also,

$$p^aH_{p^{a-1}k}=\sum_{j=1}^{p^{a-1}k}\frac{p^a}{j} \equiv \sum_{i=1}^{k}\frac{p^a}{p^{a-1}i}=pH_k \pmod{p^2}$$

for every $k=1,\dots,p-1$. Thus (5.2) implies that

$$\begin{aligned}p^{a-1}\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k}}{k} &\equiv \left(\frac{p}{3}+p^2[p=2]\right)\sum_{k=1}^{p-1}\frac{p^{2(a-1)}}{(p^{a-1}k)^2}(1+2p^aH_{p^{a-1}k})\\ &\equiv \left(\frac{p}{3}+p^2[p=2]\right)\sum_{k=1}^{p-1}\frac{1+2pH_k}{k^2} \pmod{p^3}.\end{aligned}$$

This yields (1.20) in the case $p=2$.

Now we handle the remaining case $p>3$. By the above, it suffices to show that

$$\sum_{k=1}^{p-1}\frac{1+2pH_k}{k^2} \equiv \frac{8}{3}pB_{p-3} \pmod{p^2}. \tag{5.3}$$

Let $n \in \mathbb{N}$. It is well known that

$$\sum_{j=0}^{k-1} j^n = \frac{1}{n+1}\sum_{i=0}^{n}\binom{n+1}{i}B_i k^{n+1-i} \quad \text{for } k \in \mathbb{Z}^+,$$

and that

$$\sum_{k=1}^{p-1} k^n \equiv pB_n \equiv 0 \pmod p \quad \text{if } n \not\equiv 0 \pmod{p-1}.$$

(See, e.g., [6, p. 235].) Therefore

$$\begin{aligned}\sum_{k=1}^{p-1}\frac{1}{k^2}\sum_{j=0}^{k} j^{p-2} &= \sum_{k=1}^{p-1}\left(k^{p-4} + \frac{1}{k^2(p-1)}\sum_{i=0}^{p-2}\binom{p-1}{i}B_i k^{p-1-i}\right)\\ &= \sum_{k=1}^{p-1} k^{p-4} + \frac{1}{p-1}\sum_{i=0}^{p-2}\binom{p-1}{i}B_i\sum_{k=1}^{p-1}k^{p-3-i}\\ &\equiv \binom{p-1}{p-3}B_{p-3} + \frac{B_{p-2}}{2}\sum_{k=1}^{p-1}\left(\frac{1}{k}+\frac{1}{p-k}\right) \pmod p\end{aligned}$$

and hence

$$\sum_{k=1}^{p-1}\frac{H_k}{k^2} \equiv B_{p-3} \pmod p. \tag{5.4}$$

By a result of J. W. L. Glaisher [3, 4],

$$\binom{2p-1}{p-1} \equiv 1 - p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \equiv 1 - \frac{2}{3}p^3 B_{p-3} \pmod{p^4}$$

and thus

$$\sum_{k=1}^{p-1}\frac{1}{k^2} \equiv \frac{2}{3}pB_{p-3} \pmod{p^2}. \tag{5.5}$$

Note that (5.3) follows from (5.4) and (5.5). We are done. □

References

1. R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, Math. Comp. 66(1997) 433–449.
2. G. Eisentein, Mathematische Werke, Gotthold Eisenstein, Band II, 2nd Edition, Chelsea, New York, 1989, pp. 705–711.
3. J. W. L. Glaisher, Congruences relating to the sums of product of the first n numbers and to other sums of product, Quart. J. Math. 31(1900) 1–35.

4. J. W. L. Glaisher, On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus p^2 or p^3, Quart. J. Math. 31(1900) 321–353.
5. C. Helou and G. Terjanian, On Wolstenholme's theorem and its converse, J. Number Theory 128(2008) 475–499.
6. K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory (Graduate texts in math.; 84), 2nd ed., Springer, New York, 1990.
7. E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. 39(1938) 350–360.
8. R. J. McIntosh and E. L. Roettger, A search for Fibonacci-Wieferich and Wolstenholme primes, Math. Comp. 76(2007) 2087–2094.
9. H. Pan and Z. W. Sun, A combinatorial identity with application to Catalan numbers, Discrete Math. 306(2006) 1921–1940.
10. H. C. Williams, A note on the Fibonacci quotient $F_{p-\varepsilon}/p$, Canad. Math. Bull. 25(1982) 366–370.
11. N. J. A. Sloane, Sequence A001353 in OEIS (On-Line Encyclopedia of Integer Sequences), `http://www.research.att.com/~njas/sequences/A001353`.
12. T. B. Staver, Om summasjon av potenser av binomialkoeffisienten, Norsk Mat. Tidsskrift 29(1947) 97–103.
13. Z. H. Sun and Z. W. Sun, Fibonacci numbers and Fermat's last theorem, Acta Arith. 60(1992) 371–388.
14. Z. W. Sun, A congruence for primes, Proc. Amer. Math. Soc. 123(1995) 1341–1346.
15. 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.
16. Z. W. Sun and R. Tauraso, On some new congruences for binomial coefficients, preprint, arXiv:0709.1665.