Colloq. Math. 127(2012), no. 1, 39–54.

ON SUMS OF BINOMIAL COEFFICIENTS MODULO p^2

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

Abstract. Let p be an odd prime and let a be a positive integer. In this paper we investigate the sum $\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\binom{2k}{k}/m^k \bmod p^2$, where h and m are p-adic integers with $m\not\equiv 0 \pmod p$. For example, we show that if $h\not\equiv 0 \pmod p$ and $p^a>3$, then

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\binom{2k}{k}\left(-\frac h2\right)^k\\ &\equiv\left(\frac{1-2h}{p^a}\right)\left(1+h\left(\left(4-\frac 2h\right)^{p-1}-1\right)\right) \pmod{p^2},\end{aligned}$$

where $(-)$ denotes the Jacobi symbol. Here is another remarkable congruence: If $p^a>3$ then

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

1. Introduction

Let $p>3$ be a prime. In 1828 Gauss (cf. [BEW, (9.0.1)]) proved that if $p\equiv 1 \pmod 4$ and $p=x^2+y^2$ with $x\equiv 1 \pmod 4$ and $y\equiv 0 \pmod 2$ then

$$\binom{(p-1)/2}{(p-1)/4}\equiv 2x \pmod p.$$

In 1862 J. Wolstenholme [W] established the classical congruence

$$\frac12\binom{2p}{p}=\binom{2p-1}{p-1}\equiv 1 \pmod{p^3}.$$

2010 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 11A07, 11B39, 11E25, 11S99.

Keywords. Central binomial coefficients, congruences modulo prime powers.

Supported by the National Natural Science Foundation (grant 11171140) of China and the Priority Academic Program Development of Jiangsu Higher Education Institutions.

In 1895 F. Morley [M] showed that

$$\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2}4^{p-1} \pmod{p^3}.$$

Since

$$\frac{\binom{2k}{k}}{(-4)^k} = \binom{-1/2}{k} \equiv \binom{(p-1)/2}{k} \pmod{p} \quad \text{for all } k=0,1,\ldots,p-1,$$

it is apparent that

$$\sum_{k=0}^{p-1}\binom{2k}{k} \equiv \sum_{k=0}^{(p-1)/2}\binom{(p-1)/2}{k}(-4)^k = (-3)^{(p-1)/2} \equiv \left(\frac{-3}{p}\right) \pmod{p},$$

where $(-)$ denotes the Jacobi symbol. In 2006, H. Pan and Z. W. Sun [PS] derived the congruence

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

from a sophisticated combinatorial identity. Later Sun and R. Tauraso [ST2] proved further that

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

for any $a \in \mathbb{Z}^+ = \{1,2,3,\ldots\}$. Moreover, Sun and Tauraso [ST1] determined $\sum_{k=0}^{p-1}\binom{2k}{k}/m^k \bmod p$ via the identity

$$\sum_{k=0}^{p-1}\binom{2k}{k}x^{p-1-k} = \sum_{k=0}^{p-1}\binom{2p}{k}u_{p-k}(x-2)$$

(cf. [ST1, (2.1)]), where

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

Now we need to introduce Lucas sequences.

Let $A,B \in \mathbb{Z}$. The Lucas sequences $u_n = u_n(A,B)$ $(n \in \mathbb{N} = \{0,1,2,\ldots\})$ and $v_n = v_n(A,B)$ $(n \in \mathbb{N})$ are defined by

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

and

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

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 $\Delta = A^2 - 4B$. It is well known that for any $n \in \mathbb{N}$ we have

$$u_n = \sum_{0 \leqslant k < n} \alpha^k \beta^{n-1-k} = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } \Delta \neq 0, \\ n\alpha^{n-1} = n(A/2)^{n-1} & \text{if } \Delta = 0, \end{cases}$$

and also $v_n = \alpha^n + \beta^n$. If p is a prime then

$$v_p = \alpha^p + \beta^p \equiv (\alpha + \beta)^p = A^p \equiv A \pmod{p}.$$

It is also known that

$$u_p \equiv \left(\frac{\Delta}{p}\right) \pmod{p} \quad \text{and} \quad u_{p-(\frac{\Delta}{p})} \equiv 0 \pmod{p}$$

for any prime p not dividing $2B$. (See, e.g., [S10, Lemma 2.3].) The reader may consult [S06] for connections between Lucas sequences and quadratic fields. If $A = a + 1$ and $B = a$ for some integer $a \not\equiv 0, 1 \pmod{p}$ where p is an odd prime, then $\Delta = (a-1)^2$ and

$$\frac{u_{p-(\frac{\Delta}{p})}}{p} = \frac{u_{p-1}}{p} = \frac{1}{a-1} \cdot \frac{a^{p-1} - 1}{p}.$$

In the paper [S10] the author proved that for any odd prime p and integer $m \not\equiv 0 \pmod{p}$ we have

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

See also [SSZ] and [S11a] for related results on p-adic valuations.

For a sequence $\{a_n\}_{n \geqslant 0}$ of complex numbers, its dual sequence is given by $\{a_n^*\}_{n \geqslant 0}$, where

$$a_n^* = \sum_{k=0}^{n} \binom{n}{k} (-1)^k a_k \quad (n = 0, 1, 2, \dots).$$

It is well known that $(a_n^*)^* = a_n$ for all $n \in \mathbb{N}$ (see [GKP, (5.48)] and also [S03]). Let p be an odd prime and let m be an integer not divisible by p. Clearly

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

since $\binom{p-1}{k} \equiv (-1)^k \pmod p$ for all $k = 0, 1, \ldots, p-1$. As $\sum_{k=0}^{p-1}\binom{2k}{k}/m^k$ mod p^2 has been determined, it is natural to seek for the determination of $\sum_{k=0}^{p-1}\binom{p-1}{k}\binom{2k}{k}/(-m)^k$ modulo p^2 which is the main goal of this paper.

Let p be an odd prime. When $p \equiv 3 \pmod 4$, the author [S11b] noted that

$$\sum_{k=0}^{p-1}\frac{\binom{2k}{k}^2}{8^k} \equiv 0 \pmod p$$

and conjectured further that

$$\sum_{k=0}^{p-1}\binom{p-1}{k}\frac{\binom{2k}{k}^2}{(-8)^k} \equiv 0 \pmod{p^2}.$$

In [S11b, (1.11)] it was shown that $\sum_{k=0}^{p-1}\binom{p-1}{k}\binom{2k}{k}^3/(-64)^k \equiv 0 \pmod{p^2}$ if $p > 3$ and $p \equiv 3 \pmod 4$. Inspired by these, we are led to think that it is really worth studying $\sum_{k=0}^{p-1}\binom{p-1}{k}\binom{2k}{k}/(-m)^k$ mod p^2 (with m a p–adic integer not divisible by p) which might behave better than $\sum_{k=0}^{p-1}\binom{2k}{k}/m^k$ mod p^2 in some cases.

We shall state our main results in the next section and provide some lemmas in Section 3. Section 4 is devoted to the proofs of our theorems.

2. The main results

For a prime p we use $\mathbb{Z}_p$ to denote the ring of p-adic integers; if $h \in \mathbb{Z}_p$ and $h \not\equiv 0 \pmod p$ then we denote the quotient $(h^{p-1}-1)/p \in \mathbb{Z}_p$ by $q_p(h)$ and call it a *Fermat quotient*. For $m, n \in \mathbb{N}$, the Kronecker symbol $\delta_{m,n}$ takes 1 or 0 according as $m = n$ or not.

Now we state our main results and give some corollaries.

Theorem 2.1. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. Let h be a p-adic integer with $h \not\equiv 0 \pmod p$, and ($2h \not\equiv 1 \pmod p$ or $p^a > 3$). Then*

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\binom{2k}{k}\left(-\frac{h}{2}\right)^k \\ &\equiv \left(\frac{1-2h}{p^a}\right)\left(1+h\left(\left(4-\frac{2}{h}\right)^{p-1}-1\right)\right) \pmod{p^2}.\end{aligned} \tag{2.1}$$

Corollary 2.1. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1}\binom{p^a-1}{k}\frac{\binom{2k}{k}}{(-2)^k} \equiv (-1)^{(p^a-1)/2}2^{p-1} \pmod{p^2}. \tag{2.2}$$

Proof. Simply apply Theorem 2.1 with $h=1$. □

Remark 2.1. Let $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Later we will show that

$$\begin{aligned}&\sum_{k=0}^{n-1}\binom{n-1}{k}\binom{2k}{k}(-1)^k m^{n-1-k}\\ =&\sum_{k=0}^{\lfloor (n-1)/2\rfloor}\binom{n-1}{k}\binom{n-1-k}{k}(m-2)^{n-1-2k}.\end{aligned} \tag{2.3}$$

Thus, for any prime $p>3$, by applying Morley's congruence (cf. [M], [C] and [P])

$$\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2}4^{p-1} \pmod{p^3}$$

we get

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

which is a refinement of (2.2) in the case $a=1$.

Corollary 2.2. *Let $p>3$ be a prime and let $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1}\binom{2p^a-1}{k}\binom{2k}{k}(-1)^k \equiv \left(\frac{p^a}{3}\right)(2\cdot 3^{p-1}-1) \pmod{p^2} \tag{2.4}$$

and

$$\sum_{k=0}^{p^a-1}\binom{p^a+k}{k}\frac{\binom{2k}{k}}{(-2)^k} \equiv \left(\frac{3}{p^a}\right)(1-p(q_p(2)+q_p(3))) \pmod{p^2}. \tag{2.5}$$

Proof. Just put $h=2$ and $h=-1$ in (2.1) and note that $\binom{-x}{k} = (-1)^k\binom{x+k-1}{k}$. □

Corollary 2.3. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1}\binom{2p^a+k}{k}\binom{2k}{k}(-1)^k \equiv \left(\frac{p^a}{5}\right)\left(3-2\cdot 5^{p-1}\right) \pmod{p^2}. \tag{2.6}$$

Proof. Simply apply (2.1) with $h=-2$. □

Our following result is more general than Theorem 2.1.

Theorem 2.2. *Let p be an odd prime and let $m \in \mathbb{Z}$ with $p \nmid m$. Set $\Delta = m(m-4)$ and let $h \in \mathbb{Z}_p$. Then we have*

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\frac{\binom{2k}{k}}{(-m)^k}\\ &\equiv\left(\frac{\Delta}{p^{a-1}}\right)\left(1-\frac{hm}{2}\right)u_{p-(\frac{\Delta}{p})}(m-2,1)\\ &\quad+\left(\frac{\Delta}{p^a}\right)(1+h((m-4)^{p-1}-1))\\ &\quad-\begin{cases}h(m-4)\pmod{p^2} & \text{if } p^a=3 \text{ and } 3\mid m-1,\\ 0\pmod{p^2} & \text{otherwise.}\end{cases}\end{aligned}\tag{2.7}$$

In particular, if $hm \equiv 2 \pmod p$ then

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\frac{\binom{2k}{k}}{(-m)^k}\\ &\equiv\left(\frac{\Delta}{p^a}\right)(1+h((m-4)^{p-1}-1))\\ &\quad+\begin{cases}m-4\pmod{p^2} & \text{if } p^a=3 \text{ and } 3\mid m-1,\\ 0\pmod{p^2} & \text{otherwise}\end{cases}.\end{aligned}\tag{2.8}$$

Corollary 2.4. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. If $p^a > 3$, then*

$$\sum_{k=0}^{p^a-1}\binom{p^a-1}{k}\binom{2k}{k}(-1)^k \equiv 3^{p-1}\left(\frac{p^a}{3}\right) \pmod{p^2}. \tag{2.9}$$

If $p \neq 3$, then

$$\sum_{k=0}^{p^a-1}\binom{p^a-1}{k}\frac{\binom{2k}{k}}{(-3)^k} \equiv \left(\frac{p^a}{3}\right) \pmod{p^2}. \tag{2.10}$$

Proof. Just apply (2.7) with $h = 1$ and $m \in \{1, 3\}$ and note that $(-1)^{n-1}u_n(1,1) = u_n(-1,1) = (\frac{n}{3})$ for $n \in \mathbb{N}$. $\square$

Corollary 2.5. *Let $p \neq 2, 5$ be a prime and let $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1}\binom{p^a-1}{k}\binom{2k}{k} \equiv \left(\frac{p^a}{5}\right)\left(5^{p-1}-3F_{p-(\frac{p}{5})}\right) \pmod{p^2} \tag{2.11}$$

and

$$\sum_{k=0}^{p^a-1}\binom{p^a-1}{k}\frac{\binom{2k}{k}}{(-5)^k}\equiv\left(\frac{p^a}{5}\right)\left(1-3F_{p-(\frac{p}{5})}\right)\pmod{p^2}, \tag{2.12}$$

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

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

Proof. Observe that

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

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 this, if we apply (2.7) with $h=1$ and $m\in\{-1,5\}$ then we obtain the desired result. $\square$

To conclude this section we raise four conjectures based on our computation via `Mathematica`.

Conjecture 2.1. *Let p be an odd prime and let h be an integer with $h\equiv(p+1)/2\pmod p$. If $p^a>3$ with $a\in\mathbb{Z}^+$, then*

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

Also, for any $n\in\mathbb{Z}^+$ we have

$$\frac{1}{n}\sum_{k=0}^{n-1}\binom{hn-1}{k}\binom{2k}{k}(-h/2)^k\in\mathbb{Z}_p.$$

Conjecture 2.2. *Let p be an odd prime.*

(i) *If $p\equiv 1\pmod 8$, then*

$$\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{u_k(2,-1)}{(-8)^k}\equiv\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{kv_k(2,-1)}{(-8)^k}\equiv 0\pmod{p^2}.$$

If $p\equiv 7\pmod 8$, then

$$\sum_{k=0}^{p-1}\binom{p-1}{k}\binom{2k}{k}^2\frac{u_k(2,-1)}{8^k}\equiv 0\pmod{p^2}.$$

(ii) *If* $p\equiv 1\pmod{12}$, *then*

$$\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{u_k(4,1)}{4^k}\equiv 0\pmod{p^2}.$$

If $p\equiv 11\pmod{12}$, *then*

$$\sum_{k=0}^{p-1}\binom{p-1}{k}\binom{2k}{k}^2\frac{v_k(4,1)}{(-4)^k}\equiv 0\pmod{p^2}.$$

Recall that any prime $p\equiv 1,3\pmod 8$ can be uniquely written as x^2+2y^2 with $x,y\in\mathbb{Z}^+$, and any prime $p\equiv 1\pmod 3$ can be uniquely written in the form x^2+3y^2 with $x,y\in\mathbb{Z}^+$. (See, e.g., [Co, p. 7].) The following two conjectures are related to Conjecture 2.2 and look more difficult.

Conjecture 2.3. *Let* p *be a prime with* $p\equiv 1,3\pmod 8$. *Write* $p=x^2+2y^2$ *with* $x,y\in\mathbb{Z}$ *so that* $x\equiv 1\pmod 4$, *and* $y\equiv 1\pmod 4$ *if* $p\equiv 3\pmod 8$. *Then*

$$\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{ku_k(2,-1)}{(-8)^k}\equiv\frac{p}{4x}-\frac{x}{2}\pmod{p^2}$$

and

$$\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{v_k(2,-1)}{(-8)^k}\equiv 4x-\frac{p}{x}\pmod{p^2}.$$

If $p\equiv 1\pmod 8$, *then*

$$\begin{aligned}4\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{ku_k(2,-1)}{32^k}&\equiv\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{kv_k(2,-1)}{32^k}\\&\equiv(-1)^{(p-1)/8+(x-1)/4}\left(\frac{p}{x}-2x\right)\pmod{p^2},\end{aligned}$$

and we can determine x mod p^2 *via the congruence*

$$(-1)^{(x-1)/4}x\equiv\frac{(-1)^{(p-1)/8}}{2}\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{(k+1)v_k(2,-1)}{32^k}\pmod{p^2}.$$

If $p\equiv 3\pmod 8$, *then*

$$\begin{aligned}\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{u_k(2,-1)}{(-8)^k}&\equiv(-1)^{(p-3)/8+(x-1)/4}\left(\frac{p}{2x}-2x\right)\pmod{p^2},\\ \sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{kv_k(2,-1)}{(-8)^k}&\equiv(-1)^{(p-3)/8+(x-1)/4}2\left(x+\frac{p}{x}\right)\pmod{p^2},\\ \sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{ku_k(2,-1)}{32^k}&\equiv\frac{1}{2}\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{kv_k(2,-1)}{32^k}\equiv -y\pmod{p^2},\end{aligned}$$

and

$$\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{u_k(2,-1)}{32^k}\equiv 2y-\frac{p}{4y}\pmod{p^2}.$$

Conjecture 2.4. *Let $p>3$ be a prime.*

(i) *If $p\equiv 1\pmod{12}$ and $p=x^2+3y^2$ with $x,y\in\mathbb{Z}$ and $x\equiv 1\pmod 4$, then*

$$\begin{aligned}&(-1)^{(p-1)/4}\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{v_k(4,1)}{4^k}\\ \equiv&\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{v_k(4,1)}{64^k}\equiv 4x-\frac{p}{x}\pmod{p^2},\end{aligned}$$

also we can determine x mod p^2 by

$$\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{(k+2)v_k(4,1)}{4^k}\equiv(-1)^{(p-1)/4}4x\pmod{p^2}$$

as well as

$$\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{(k-1)v_k(4,1)}{64^k}\equiv -2x\pmod{p^2}.$$

(ii) *If $p\equiv 7\pmod{12}$ and $p=x^2+3y^2$ with $x,y\in\mathbb{Z}$ and $y\equiv 1\pmod 4$, then*

$$\begin{aligned}\sum_{k=0}^{p-1}\frac{u_k(4,1)}{64^k}\binom{2k}{k}^2\equiv&2y-\frac{p}{6y}\pmod{p^2},\\ \sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{u_k(4,1)}{4^k}\equiv&(-1)^{(p+1)/4}\left(4y-\frac{p}{3y}\right)\pmod{p^2},\\ \sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{v_k(4,1)}{4^k}\equiv&(-1)^{(p-3)/4}\left(12y-\frac{p}{y}\right)\pmod{p^2},\\ \sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{kv_k(4,1)}{4^k}\equiv&(-1)^{(p+1)/4}\left(20y-\frac{8p}{y}\right)\pmod{p^2},\end{aligned}$$

and also

$$\begin{aligned}y\equiv&\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{ku_k(4,1)}{64^k}\equiv\frac{1}{4}\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{kv_k(4,1)}{64^k}\\ \equiv&\frac{(-1)^{(p+1)/4}}{22}\sum_{k=0}^{p-1}\binom{2k}{k}^2\frac{(k+7)u_k(4,1)}{4^k}\pmod{p^2}.\end{aligned}$$

3. Some Lemmas

Recall that harmonic numbers H_n ($n \in \mathbb{N}$) are defined by $H_n = \sum_{0<k\leqslant n} 1/k$. The reader may consult [S12a] and [S12b] for some fundamental congruences involving harmonic numbers.

Lemma 3.1. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. Let $m \in \mathbb{Z}$ with $p \nmid m$. If $p \mid m-4$ then*

$$\sum_{k=1}^{p^a-1} \frac{p^{a-1}H_k}{m^k}\binom{2k}{k} \equiv 2\delta_{a,1} \pmod{p}. \tag{3.1}$$

When $m \not\equiv 4 \pmod{p}$, we have

$$\sum_{k=1}^{p^a-1} \frac{p^{a-1}H_k}{m^k}\binom{2k}{k} \equiv -\left(\frac{m(m-4)}{p^a}\right)\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k(4-m)^k} \pmod{p}. \tag{3.2}$$

Proof. For $k = 1, \ldots, (p^a-1)/2$, we have

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

If $k \in \{(p^a+1)/2, \ldots, p^a-1\}$, then $2k-p^a \in \{1, \ldots, k-1\}$ and hence

$$\binom{2k}{k} = \binom{p^a+(2k-p^a)}{k} \equiv \binom{p^a}{0}\binom{2k-p^a}{k} = 0 \pmod{p}$$

with the help of Lucas' congruence (cf. [St, p. 44]). So, for any $k = 0, \ldots, p^a-1$ we have

$$\binom{2k}{k} \equiv (-4)^k\binom{(p^a-1)/2}{k} \pmod{p}. \tag{3.3}$$

Therefore

$$\sum_{k=1}^{p^a-1} \frac{p^{a-1}H_k}{m^k}\binom{2k}{k} \equiv \sum_{k=1}^{(p^a-1)/2}\binom{(p^a-1)/2}{k}(-4/m)^k\,(p^{a-1}H_k) \pmod{p}.$$

(Note that $p^{a-1}H_k = \sum_{j=1}^{k} p^{a-1}/j \in \mathbb{Z}_p$ for every $k = 1, \ldots, p^a-1$.)

For each $k\in\mathbb{N}$ clearly

$$\begin{aligned}H_k=\sum_{0<j\leqslant k}\int_0^1 x^{j-1}dx&=\int_0^1\sum_{0<j\leqslant k}x^{j-1}dx\\&=\int_0^1\frac{1-x^k}{1-x}dx=\int_0^1\frac{1-(1-t)^k}{t}dt.\end{aligned}$$

Thus

$$\sum_{k=1}^{p^a-1}\frac{p^{a-1}H_k}{m^k}\binom{2k}{k}\equiv p^{a-1}\Sigma\pmod p,$$

where

$$\begin{aligned}\Sigma:=&\int_0^1\sum_{k=0}^{(p^a-1)/2}\binom{(p^a-1)/2}{k}\left(-\frac{4}{m}\right)^k\frac{1-(1-t)^k}{t}dt\\=&\int_0^1\frac{(1-4/m)^{(p^a-1)/2}-(1-(1-t)4/m)^{(p^a-1)/2}}{t}dt\\=&-\sum_{k=1}^{(p^a-1)/2}\binom{(p^a-1)/2}{k}\left(1-\frac{4}{m}\right)^{(p^a-1)/2-k}\int_0^1\left(\frac{4t}{m}\right)^k\frac{dt}{t}\\=&-\frac{1}{m^{(p^a-1)/2}}\sum_{k=1}^{(p^a-1)/2}\binom{(p^a-1)/2}{k}\frac{4^k}{k}(m-4)^{(p^a-1)/2-k}.\end{aligned}$$

If $m\equiv 4\pmod p$, then

$$p^{a-1}\Sigma=-\frac{1}{m^{(p^a-1)/2}}\cdot\frac{p^{a-1}}{(p^a-1)/2}4^{(p^a-1)/2}\equiv 2\delta_{a,1}\pmod p$$

and hence (3.1) holds.

Now assume that $m\not\equiv 4\pmod p$. In view of (3.3),

$$\begin{aligned}p^{a-1}\Sigma\equiv&-\frac{(m(m-4))^{(p^a-1)/2}}{m^{p^a-1}}\sum_{k=1}^{p^a-1}\binom{2k}{k}\frac{(-1)^kp^{a-1}}{k(m-4)^k}\\\equiv&-\left(\frac{m(m-4)}{p^a}\right)p^{a-1}\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k}}{k(4-m)^k}\pmod p.\end{aligned}$$

So it suffices to prove that

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

for any $n\in\mathbb{Z}$ with $p\nmid n$. If $p^{a-1}\nmid k$ then $p^{a-1}/k\equiv 0\pmod p$. Therefore

$$p^{a-1}\sum_{k=1}^{p^a-1}\frac{\binom{2k}{k}}{kn^k}\equiv p^{a-1}\sum_{j=1}^{p-1}\frac{\binom{2p^{a-1}j}{p^{a-1}j}}{p^{a-1}jn^{p^{a-1}j}}\equiv\sum_{j=1}^{p-1}\frac{\binom{2j}{j}}{jn^j}\pmod p$$

in view of the Lucas congruence. □

Lemma 3.2 (Sun [S10]). *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*

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

Lemma 3.3 (Sun and Tauraso [ST1, Theorem 1.2]). *Let p be any prime and let m be an integer not divisible by p. Then we have*

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

Lemma 3.4. *Let p be an odd prime and let $m\in\mathbb{Z}$ with $\Delta=m(m-4)\not\equiv 0\pmod{p}$. Then*

$$\begin{aligned}&\frac{2}{m-4}\cdot\frac{v_p(m-4,4-m)-(m-4)^p}{p}\\ \equiv&\frac{m}{2}\left(\frac{\Delta}{p}\right)\frac{u_{p-(\frac{\Delta}{p})}(m-2,1)}{p}-q_p(m-4)\pmod{p}.\end{aligned}\tag{3.4}$$

Proof. (i) Let us first show the equality

$$\frac{v_{2n+1}(m-4,4-m)}{(m-4)^{n+1}}=\frac{u_{2n+1}(m,m)}{m^n}\tag{3.5}$$

for $n=0,1,2,\ldots$. Clearly both sides of (3.5) coincide with 1 when $n=0$. Note that

$$\begin{aligned}\frac{v_3(m-4,4-m)}{(m-4)^2}=&\frac{v_2(m-4,4-m)+v_1(m-4,4-m)}{m-4}\\ =&v_1(m-4,4-m)+v_0(m-4,4-m)+\frac{v_1(m-4,4-m)}{m-4}\\ =&m-4+2+1=m-1=u_2(m,m)-u_1(m,m)=\frac{u_3(m,m)}{m}.\end{aligned}$$

Also, for $n=2,3,\ldots$ we have

$$\begin{aligned}&\frac{v_{2n+1}(m-4,4-m)}{(m-4)^{n+1}}\\ =&\frac{v_{2n-1}(m-4,4-m)+v_{2n}(m-4,4-m)}{(m-4)^n}\\ =&\frac{(1+(m-4))v_{2n-1}(m-4,4-m)+(m-4)v_{2n-2}(m-4,4-m)}{(m-4)^n}\\ =&\frac{(m-2)v_{2n-1}(m-4,4-m)-(m-4)v_{2n-3}(m-4,4-m)}{(m-4)^n}\\ =&(m-2)\frac{v_{2n-1}(m-4,4-m)}{(m-4)^n}-\frac{v_{2n-3}(m-4,4-m)}{(m-4)^{n-1}}\end{aligned}$$

and

$$\begin{aligned}\frac{u_{2n+1}(m,m)}{m^n} =&\frac{u_{2n}(m,m)-u_{2n-1}(m,m)}{m^{n-1}}\\ =&\frac{(m-1)u_{2n-1}(m,m)-mu_{2n-2}(m,m)}{m^{n-1}}\\ =&\frac{(m-1)u_{2n-1}(m,m)-(u_{2n-1}(m,m)+mu_{2n-3}(m,m))}{m^{n-1}}\\ =&(m-2)\frac{u_{2n-1}(m,m)}{m^{n-1}}-\frac{u_{2n-3}(m,m)}{m^{n-2}}.\end{aligned}$$

Thus, by induction (3.5) holds for all $n\in\mathbb{N}$.

(ii) By part (i),

$$u_p(m,m)=\frac{m^{(p-1)/2}}{(m-4)^{(p+1)/2}}(v_p(m-4,4-m)-(m-4)^p)+(m(m-4))^{(p-1)/2}.$$

Since $v_p(m-4,4-m)\equiv(m-4)^p \pmod p$ and

$$\begin{aligned}&\Delta^{(p-1)/2}-\left(\frac{\Delta}{p}\right)\\ =&(m-4)^{(p-1)/2}\left(m^{(p-1)/2}-\left(\frac{m}{p}\right)\right)+\left(\frac{m}{p}\right)\left((m-4)^{(p-1)/2}-\left(\frac{m-4}{p}\right)\right)\\ \equiv&\left(\frac{\Delta}{p}\right)\left(\frac{m}{p}\right)\left(m^{(p-1)/2}-\left(\frac{m}{p}\right)\right)\\ &+\left(\frac{\Delta}{p}\right)\left(\frac{m-4}{p}\right)\left((m-4)^{(p-1)/2}-\left(\frac{m-4}{p}\right)\right)\\ \equiv&\frac{1}{2}\left(\frac{\Delta}{p}\right)\left(m^{p-1}-1+(m-4)^{p-1}-1\right) \pmod{p^2},\end{aligned}$$

we have

$$\begin{aligned}u_p(m,m)-\left(\frac{\Delta}{p}\right)\equiv&\frac{(\frac{m}{p})}{(m-4)(\frac{m-4}{p})}(v_p(m-4,4-m)-(m-4)^p)\\ &+\frac{1}{2}\left(\frac{\Delta}{p}\right)\left(m^{p-1}-1+(m-4)^{p-1}-1\right)\\ \equiv&\frac{1}{m-4}\left(\frac{\Delta}{p}\right)(v_p(m-4,4-m)-(m-4)^p)\\ &+\frac{p}{2}\left(\frac{\Delta}{p}\right)(q_p(m)+q_p(m-4)) \pmod{p^2}.\end{aligned}$$

On the other hand, by [S10, Lemma 2.4] we have

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

Thus

$$\begin{aligned}&\frac{2}{m-4}\left(\frac{\Delta}{p}\right)(v_p(m-4,4-m)-(m-4)^p)\\ \equiv& u_p(m-2,1)-\left(\frac{\Delta}{p}\right)+u_{p-(\frac{\Delta}{p})}(m-2,1)-\left(\frac{\Delta}{p}\right)p\,q_p(m-4)\pmod{p^2}.\end{aligned}$$

In view of this, we have reduced (3.4) to the following congruence

$$u_p(m-2,1)-\left(\frac{\Delta}{p}\right)\equiv\left(\frac{m}{2}-1\right)u_{p-(\frac{\Delta}{p})}(m-2,1)\pmod{p^2}. \tag{3.6}$$

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

$$v_n(m-2,1)^2-\Delta u_n^2(m-2,1)=(\alpha^n+\beta^n)^2-(\alpha^n-\beta^n)^2=4(\alpha\beta)^n=4$$

for all $n\in\mathbb{N}$. As $u_{p-(\frac{\Delta}{p})}(m-2,1)\equiv 0\pmod p$ we have

$$v_{p-(\frac{\Delta}{p})}(m-2,1)^2-4\equiv 0\pmod{p^2}.$$

By [S10, Lemma 2.3], $v_{p-(\frac{\Delta}{p})}(m-2,1)\equiv 2\pmod p$. So

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

By induction, $(m-2)u_n(m-2,1)\pm v_n(m-2,1)=2u_{n\pm1}(m-2,1)$ for all $n\in\mathbb{Z}^+$. Therefore

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

and hence (3.6) follows.

The proof of Lemma 3.4 is now complete. □

Combining Lemmas 3.3 and 3.4 we get the following result.

Lemma 3.5. *Let p be an odd prime and let $m\in\mathbb{Z}$ with $\Delta=m(m-4)\not\equiv 0\pmod p$. Then*

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k(m-4)^k}\equiv q_p(m-4)-\frac{m}{2}\left(\frac{\Delta}{p}\right)\frac{u_{p-(\frac{\Delta}{p})}(m-2,1)}{p}\pmod p. \tag{3.7}$$

4. Proofs of Theorems 2.1–2.2 and (2.3)

Proof of Theorem 2.2. For $k=0,\ldots,p^a-1$, clearly

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

Thus

$$\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\frac{\binom{2k}{k}}{(-m)^k}\equiv\sum_{k=0}^{p^a-1}\frac{\binom{2k}{k}}{m^k}-hp^a\sum_{k=0}^{p^a-1}\frac{H_k}{m^k}\binom{2k}{k} \pmod{p^2}$$

and hence

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\frac{\binom{2k}{k}}{(-m)^k}+hp^a\sum_{k=0}^{p^a-1}\frac{H_k}{m^k}\binom{2k}{k}\\ &\equiv\left(\frac{\Delta}{p^a}\right)+\left(\frac{\Delta}{p^{a-1}}\right)u_{p-(\frac{\Delta}{p})}(m-2,1) \pmod{p^2}\end{aligned}\tag{4.1}$$

with the help of Lemma 3.2.

If $p\nmid m-4$, then by combining (4.1), (3.2) and Lemma 3.5 we get

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\binom{hp^a-1}{k}\frac{\binom{2k}{k}}{(-m)^k}\\ \equiv&\left(\frac{\Delta}{p^a}\right)+\left(\frac{\Delta}{p^{a-1}}\right)u_{p-(\frac{\Delta}{p})}(m-2,1)\\ &+ph\Bigg(\left(\frac{\Delta}{p^a}\right)q_p(m-4)-\frac{m}{2}\left(\frac{\Delta}{p^{a-1}}\right)\frac{u_{p-(\frac{\Delta}{p})}(m-2,1)}{p}\Bigg) \pmod{p^2}\end{aligned}$$

and hence (2.7) follows. (Note that if $p^a=3$ and $3\mid m-1$ then $m\equiv 4 \pmod p$.) In the case $m\equiv 4 \pmod p$, we have

$$p^a\sum_{k=1}^{p^a-1}\frac{H_k}{m^k}\binom{2k}{k}\equiv 2p\delta_{a,1} \pmod{p^2}$$

by (3.1), and

$$\begin{aligned}&u_{p-(\frac{\Delta}{p})}(m-2,1)=u_p(m-2,1)\\ \equiv&p\left(\frac{m-2}{2}\right)^{p-1}+\delta_{p,3}\,pm\frac{m-4}{3}\equiv p+\delta_{p,3}(m-4) \pmod{p^2}\end{aligned}$$

by [S11a, Lemma 2.2]. So (4.1) also implies (2.7) when $p \mid m-4$.

Since $u_{p-(\frac{\Delta}{p})}(m-2,1) \equiv 0 \pmod p$ by [S10, Lemma 2.3], (2.7) in the case $hm \equiv 2 \pmod p$ yields (2.8).

So far we have completed the proof of Theorem 2.2. $\Box$

Proof of Theorem 2.1. Choose $m \in \mathbb{Z}$ such that $hm \equiv 2 \pmod{p^2}$. Clearly $p \nmid m$. Note that

$$m-4 \equiv \frac{2}{h}-4=\frac{2-4h}{h} \pmod{p^2}.$$

So we may get (2.1) by applying (2.8). This concludes the proof of Theorem 2.1. $\Box$

Proof of (2.3). For $k \in \mathbb{N}$ clearly the constant term of

$$(2-x-x^{-1})^k=\frac{(-1)^k}{x^k}(x-1)^{2k}$$

is the central binomial coefficient $\binom{2k}{k}$. Observe that

$$\sum_{k=0}^{n-1}\binom{n-1}{k}(-1)^k m^{n-1-k}(2-x-x^{-1})^k=(m-2+x+x^{-1})^{n-1}.$$

Comparing the constant terms of both sides of the last equality we obtain

$$\begin{aligned}&\sum_{k=0}^{n-1}\binom{n-1}{k}\binom{2k}{k}(-1)^k m^{n-1-k}\\=&\sum_{k=0}^{\lfloor (n-1)/2\rfloor}\binom{n-1}{k,k,n-1-2k}(m-2)^{n-1-2k},\end{aligned}$$

which is equivalent to (2.3). $\Box$

Acknowledgment. The author would like to thank the referee for helpful comments.

References

[BEW] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, 1998.

[C] L. Calitz, *A theorem of Glaisher*, Canad. J. Math. **5** (1953), 306–316.

[Co] D. A. Cox, *Primes of the Form* x^2+ny^2, John Wiley & Sons, 1989.

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

[M] F. Morley, *Note on the congruence* $2^{4n} \equiv (-1)^n(2n)!/(n!)^2$, *where* $2n+1$ *is a prime*, Ann. Math. **9** (1895), 168–170.

[P] H. Pan, *On a generalization of Carlitz's congruence*, Int. J. Mod. Math. **4** (2009), 87–93.

[PS] H. Pan and Z. W. Sun, *A combinatorial identity with application to Catalan numbers*, Discrete Math. **306** (2006), 1921–1940.

[St] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, Cambridge Univ. Press, Cambridge, 1999.

[SSZ] N. Strauss, J. Shallit and D. Zagier, *Some strange* 3*-adic identities*, Amer. Math. Monthly **99** (1992), 66–69.

[SS] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371–388.

[S03] Z. W. Sun, *Combinatorial identities in dual sequences*, European J. Combin. **24** (2003), 709–718.

[S06] Z. W. Sun, *Binomial coefficients and quadratic fields*, Proc. Amer. Math. Soc. **134** (2006), 2213–2222.

[S10] Z. W. Sun, *Binomial coefficients, Catalan numbers and Lucas quotients*, Sci. China Math. **53** (2010), 2473–2488. `http://arxiv.org/abs/0909.5648`.

[S11a] Z. W. Sun, *p-adic valuations of some sums of multinomial coefficients*, Acta Arith. **148** (2011), 63–76.

[S11b] Z. W. Sun, *On congruences related to central binomial coefficients*, J. Number Theory **131** (2011), 2219–2238.

[S12a] Z. W. Sun, *Arithmetic theory of harmonic numbers*, Proc. Amer. Math. Soc. **140** (2012), 415–428.

[S12b] Z. W. Sun, *On harmonic numbers and Lucas sequences*, Publ. Math. Debrecen **80** (2012), 25–41.

[ST1] Z. W. Sun and R. Tauraso, *New congruences for central binomial coefficients*, Adv. in Appl. Math. **45** (2010), 125–148.

[ST2] Z. W. Sun and R. Tauraso, *On some new congruences for binomial coefficients*, Int. J. Number Theory **7** (2011), 645–662.

[W] J. Wolstenholme, *On certain properties of prime numbers*, Quart. J. Appl. Math. **5** (1862), 35–39.