Preprint, arXiv:0909.3808

arXiv:0909.3808v2 [math.NT] 28 Sep 2009

VARIOUS CONGRUENCES INVOLVING BINOMIAL COEFFICIENTS AND HIGHER-ORDER CATALAN NUMBERS

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 a prime and let a be a positive integer. In this paper we investigate $\sum_{k=0}^{p^a-1}\binom{(h+1)k}{k+d}/m^k$ modulo a prime p, where d and m are integers with $-h<d\leqslant p^a$ and $m\not\equiv 0 \pmod p$. We also study congruences involving higher-order Catalan numbers $C_k^{(h)}=\frac{1}{hk+1}\binom{(h+1)k}{k}$ and $\bar C_k^{(h)}=\frac{h}{k+1}\binom{(h+1)k}{k}$. Our tools include linear recurrences and the theory of cubic residues. Here are some typical results in the paper. (i) If $p^a\equiv 1 \pmod 6$ then

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k}}{6^k}\equiv 2^{(p^a-1)/3}\pmod p\quad\text{and}\quad\sum_{k=1}^{p^a-1}\frac{\bar C_k^{(2)}}{6^k}\equiv 0\pmod p.$$

Also,

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k}}{7^k}\equiv\begin{cases}-2&\text{if }p^a\equiv\pm2\pmod 7,\\1&\text{otherwise.}\end{cases}$$

(ii) We have

$$\sum_{k=0}^{p^a-1}\frac{\binom{4k}{k}}{5^k}\equiv\begin{cases}1\pmod p&\text{if }p\neq 11\text{ and }p^a\equiv 1\pmod 5,\\-1/11\pmod p&\text{if }p^a\equiv 2,3\pmod 5,\\-9/11\pmod p&\text{if }p^a\equiv 4\pmod 5.\end{cases}$$

Also,

$$\sum_{k=0}^{p^a-1}\frac{C_k^{(3)}}{5^k}\equiv\begin{cases}1\pmod p&\text{if }p^a\equiv 1,3\pmod 5,\\-2\pmod p&\text{if }p^a\equiv 2\pmod 5,\\0\pmod p&\text{if }p^a\equiv 4\pmod 5.\end{cases}$$

2010 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 11A07.
Supported by the National Natural Science Foundation (grant 10871087) and the Overseas Cooperation Fund (grant 10928101) of China.

1. Introduction

Let p be a prime. Via a sophisticated combinatorial identity, H. Pan and Z. W. Sun [PS] proved that

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

where $(-)$ is the Jacobi symbol. Let $a\in\mathbb{Z}^+=\{1,2,3,\ldots\}$ and $d\in\{0,\ldots,p^a\}$. Recently Sun and R. Tauraso [ST1] used a new approach to determine $\sum_{k=0}^{p^a-1}\binom{2k}{k+d}\bmod p^2$; they [ST2] also studied $\sum_{k=1}^{p^a-1}\binom{2k}{k+d}/m^k$ modulo p via Lucase sequences, where m is an integer not divisible by p.

Quite recently, L. Zhao, Pan and Sun [ZPS] proved that if $p\neq 2,5$ is a prime then

$$\sum_{k=1}^{p-1}2^k\binom{3k}{k}\equiv\frac{6}{5}\left(\left(\frac{-1}{p}\right)-1\right)\pmod p$$

and

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

where $C_k^{(2)}=\binom{3k}{k}/(2k+1)$ $(k\in\mathbb{N}=\{0,1,2,\ldots\})$ are Catalan numbers of order 2.

In general, (the first-kind) Catalan numbers of order $h\in\mathbb{Z}^+$ are given by

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

(As usual, $\binom{x}{-n}=0$ for $n=1,2,\ldots$.) We also define the second-kind Catalan numbers of order h as follows:

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

Those $C_k=C_k^{(1)}=\bar{C}_k^{(1)}$ are ordinary Catalan numbers which have lots of combinatorial interpretations (see, e.g., Stanley [St]).

Let p be a prime and a a positive integer. In this paper we mainly investigate $\sum_{k=0}^{p^a-1}\binom{3k}{k}/m^k\bmod p$ for all $m\in\mathbb{Z}$ with $m\not\equiv 0\pmod p$, and determine $\sum_{k=0}^{p^a-1}\binom{4k}{k}/5^k$ and $\sum_{k=0}^{p^a-1}C_k^{(3)}/5^k$ modulo p. Our approach involves third-order and fourth order recurrences and the theory of cubic residues.

Now we introduce some basic notations throughout this paper. For a positive integer n, we use $\mathbb{Z}_n$ to denote the set of all rational numbers whose denominators are relatively prime to n. Thus, if p is a prime then $\mathbb{Z}_p$ is the ring of rational p-adic integers. For a predicate P, we let

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

Thus $[m=n]$ coincides with the Kronecker $\delta_{m,n}$.

Our first theorem is a further extension of the above-mentioned congruences of Zhao, Pan and Sun.

Theorem 1.1. *Let p be an odd prime and let $a\in\mathbb{Z}^+$. Let $c\in\mathbb{Z}_p$ with $c\not\equiv 0,-1,2 \pmod p$, and set $c'=3/(2(c+1)(c-2))$. Then*

$$\sum_{k=1}^{p^a-1}\frac{c^{2k}}{(c+1)^{3k}}\binom{3k}{k}\equiv c'\left(1-\left(\frac{4c+1}{p^a}\right)\right) \pmod p,$$

$$\sum_{k=1}^{p^a-1}\frac{c^{2k+1}}{(c+1)^{3k}}\binom{3k}{k-1}\equiv (c'+1)\left(1-\left(\frac{4c+1}{p^a}\right)\right) \pmod p,$$

$$\sum_{k=1}^{p^a-1}\frac{c^{2k+2}}{(c+1)^{3k}}\binom{3k}{k+1}\equiv (c'(3c+2)+1)\left(1-\left(\frac{4c+1}{p^a}\right)\right) \pmod p,$$

and

$$\sum_{k=0}^{p^a-1}\frac{c^{2k}}{(c+1)^{3k}}\binom{3k}{k+p^a}\equiv cc'\left(\left(\frac{4c+1}{p^a}\right)-1\right) \pmod p.$$

Remark 1.1. Note that if $c=-1/4$ then $c^2/(c+1)^3=2^2/(2+1)^3$.

Clearly Theorem 1.1 in the case $c=-1/2$ yields the two congruences of Zhao, Pan and Sun [ZPS] mentioned above. Applying Theorem 1.1 with $c=1,-2$ we obtain the following consequence.

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

$$\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k}}{8^k}\equiv\frac{3}{4}\left(\left(\frac{p^a}{5}\right)-1\right) \pmod p,$$

$$\sum_{k=1}^{p^a-1}\frac{C_k^{(2)}}{8^k}\equiv\frac{5}{4}\left(\left(\frac{p^a}{5}\right)-1\right) \pmod p,$$

$$\sum_{k=1}^{p^a-1}(-4)^k\binom{3k}{k}\equiv\frac{3}{8}\left(1-\left(\frac{p^a}{7}\right)\right) \pmod p,$$

$$\sum_{k=1}^{p^a-1}(-4)^kC_k^{(2)}\equiv\frac{7}{4}\left(1-\left(\frac{p^a}{7}\right)\right) \pmod p.$$

For a polynomial

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=\prod_{i=1}^n(x-\alpha_i)\in\mathbb{C}[x],$$

its discriminant is defined by

$$D(f)=\prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)^2.$$

By Vitae's theorem and the fundamental theorem of symmetric polynomials, we can express $D(f)$ as a rational expression involving the coefficients $a_1,\ldots,a_n$. For example, it is known that

$$D(x^3+a_1x^2+a_2x+a_3)=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3.$$

If $f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in\mathbb{Z}[x]$ and p is an odd prime not dividing $D(f)$, then

$$\left(\frac{D(f)}{p}\right)=(-1)^{n-r}$$

by Stickelberger's theorem (cf. [C]), where r is the total number of monic irreducible factors of $f(x)$ modulo p.

Let p be an odd prime and m an integer with $m\not\equiv 0,27/4 \pmod p$. Then $D=D((x+1)^3-3x^2)=(4m-27)m^2\not\equiv 0 \pmod p$. Suppose that there is no $c\in\mathbb{Z}_p$ such that $mc^2\equiv(c+1)^3 \pmod p$. Then the polynomial $(1+x)^3-mx^2$ is irreducible modulo p, hence by the Stickelberger theorem we have $(\frac{D}{p})=(-1)^{3-1}=1$. Thus $(\frac{4m-27}{p})=1$, and hence $4m-27\equiv(2t+1)^2 \pmod p$ for some $t\in\mathbb{Z}$. Note that $m\equiv t^2+t+7 \pmod p$.

The following theorem deals with the case $m=6$ and $(\frac{4m-27}{p})=1$.

Theorem 1.2. *Let $p>3$ be a prime and let $a\in\mathbb{Z}^+$. Suppose that $p^a\equiv 1 \pmod 6$. Then*

$$\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k}}{6^k(k+1)}\equiv\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k-1}}{6^k}\equiv 0 \pmod p$$

and

$$\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k}}{6^k}\equiv 2^{(p^a-1)/3}-1\equiv\frac12\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k+1}}{6^k} \pmod p.$$

Now we need to introduce another notation. For a positive integer $n\not\equiv 0 \pmod 3$ and $i\in\{0,1,2\}$, Z.-H. Sun [S98] investigated

$$C_i(n)=\left\{k\in\mathbb{Z}_n:\ \left(\frac{k+1+2\omega}{n}\right)_3=\omega^i\right\},$$

where ω is the primitive cubic root $(-1+\sqrt{-3})/2$ of unity, and $(\frac{\cdot}{n})_3$ is the cubic Jacobi symbol. (The reader is referred to Chapter 9 of [IR, pp. 108-137] for the basic theory of cubic residues.) By [S98], $k \in C_2(n)$ if and only if $-k \in C_1(n)$; also

$$C_0(n) \cup C_1(n) \cup C_2(n) = \{k \in \mathbb{Z}_n : \ k^2+3 \text{ is relatively prime to } n\}.$$

Theorem 1.3. *Let $p > 3$ be a prime and let $a \in \mathbb{Z}^+$. Let $m, t \in \mathbb{Z}_p$ with $t \not\equiv -1/2 \pmod p$ and $m \equiv t^2+t+7 \not\equiv 0, 6 \pmod p$. Then*

$$c = \frac{2m^2-18m+27}{6t+3} \in C_0(p^a) \cup C_1(p^a) \cup C_2(p^a).$$

If $c \in C_0(p^a)$, then

$$\sum_{k=1}^{p^a-1} \frac{\binom{3k}{k+d}}{m^k} \equiv 0 \pmod p \quad \text{for } d \in \{0, \pm 1\},$$

and hence

$$\sum_{k=1}^{p^a-1} \frac{C_k^{(2)}}{m^k} \equiv \sum_{k=1}^{p^a-1} \frac{\bar{C}_k^{(2)}}{m^k} \equiv 0 \pmod p.$$

When $\pm c \in C_1(p^a)$, we have

$$\sum_{k=1}^{p^a-1} \frac{\binom{3k}{k+d}}{m^k} \equiv \begin{cases} (\pm 3/(2t+1)-3)/2 \pmod p & \text{if } d=0, \\ \pm(m-6)/(2t+1) \pmod p & \text{if } d=-1, \\ \pm 3/(2t+1)+3-m \pmod p & \text{if } d=1, \end{cases}$$

and hence

$$\sum_{k=1}^{p^a-1} \frac{\bar{C}_k^{(2)}}{m^k} \equiv m-6 \pmod p.$$

Remark 1.2. Let $p > 3$ be a prime. By [S98, Corollary 6.1], if $c \in \mathbb{Z}_p$ and $c(c^2+3) \not\equiv 0 \pmod p$, then $c \in C_0(p) \iff u_{(p-(\frac{p}{3}))/3} \equiv 0 \pmod p$, where $u_0 = 0$, $u_1 = 1$, and $u_{n+1} = 6u_n - (3c^2+9)u_{n-1}$ for $n \in \mathbb{Z}^+$.

Combining Theorems 1.1-1.3 we obtain the following somewhat surprising result.

Theorem 1.4. *Let $p > 3$ be a prime. Let a be a positive integer divisible by 6 and let $d \in \{0, \pm 1\}$. Then*

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

for all $r\in\mathbb{Z}$, and hence

$$\sum_{k=1}^{p^a-1}\binom{3k}{k+d}\equiv-[p=23]3\times 2^{d+1}\pmod p.$$

We may apply Theorem 1.3 to some particular integers $m=t^2+t+7$ to obtain concrete results.

Theorem 1.5. *Let $p\neq 3$ be a prime and let $a\in\mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k}}{9^k}\equiv\begin{cases}1 & \text{if } p^a\equiv\pm1\pmod 9,\\ 0 & \text{if } p^a\equiv\pm2\pmod 9,\\ -1 & \text{if } p^a\equiv\pm4\pmod 9;\end{cases}$$

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k-1}}{9^k}\equiv\begin{cases}0 & \text{if } p^a\equiv\pm1\pmod 9,\\ 1 & \text{if } p^a\equiv\pm2\pmod 9,\\ -1 & \text{if } p^a\equiv\pm4\pmod 9;\end{cases}$$

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k+1}}{9^k}\equiv\begin{cases}0 & \text{if } p^a\equiv\pm1\pmod 9,\\ -5 & \text{if } p^a\equiv\pm2\pmod 9,\\ -7 & \text{if } p^a\equiv\pm4\pmod 9.\end{cases}$$

Consequently,

$$\sum_{k=1}^{p^a-1}\frac{C_k^{(2)}}{9^k}\equiv-3[p^a\equiv\pm2\ (\mathrm{mod}\ 9)]\pmod p$$

and

$$\sum_{k=1}^{p^a-1}\frac{\bar{C}_k^{(2)}}{9^k}\equiv 3[p^a\not\equiv\pm1\ (\mathrm{mod}\ 9)]\pmod p.$$

Theorem 1.6. *Let $p\neq 7$ be a prime and let $a\in\mathbb{Z}^+$. Then*

$$\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k}}{7^k}\equiv-3[p^a\equiv\pm2\ (\mathrm{mod}\ 7)]\pmod p;$$

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k-1}}{7^k}\equiv\begin{cases}0 & \text{if } p^a\equiv\pm1\pmod 7,\\ -1 & \text{if } p^a\equiv\pm2\pmod 7,\\ 1 & \text{if } p^a\equiv\pm3\pmod 7;\end{cases}$$

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k+1}}{7^k}\equiv\begin{cases}0 & \text{if } p^a\equiv\pm1\pmod 7,\\ -7 & \text{if } p^a\equiv\pm2\pmod 7,\\ -1 & \text{if } p^a\equiv\pm3\pmod 7.\end{cases}$$

Consequently,

$$\sum_{k=0}^{p^a-1}\frac{C_k^{(2)}}{7^k}\equiv\begin{cases}1 \pmod p & \text{if } p^a\equiv\pm1 \pmod 7,\\ 0 \pmod p & \text{if } p^a\equiv\pm2 \pmod 7,\\ -1 \pmod p & \text{if } p^a\equiv\pm3 \pmod 7;\end{cases}$$

and

$$\sum_{k=1}^{p^a-1}\frac{\bar{C}_k^{(2)}}{7^k}\equiv[p^a\not\equiv\pm1 \pmod 7] \pmod p.$$

Theorem 1.7. *Let p be a prime and let $a\in\mathbb{Z}^+$. If $p\neq5,13$, then*

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k}}{13^k}\equiv\begin{cases}1 \pmod p & \text{if } p^a\equiv\pm1,\pm5 \pmod{13},\\ -4/5 \pmod p & \text{if } p^a\equiv\pm2,\pm3 \pmod{13},\\ -1/5 \pmod p & \text{if } p^a\equiv\pm4,\pm6 \pmod{13},\end{cases}$$

and

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k+1}}{13^k}\equiv\begin{cases}1 \pmod p & \text{if } p^a\equiv\pm1,\pm5 \pmod{13},\\ -53/5 \pmod p & \text{if } p^a\equiv\pm2,\pm3 \pmod{13},\\ -47/5 \pmod p & \text{if } p^a\equiv\pm4,\pm6 \pmod{13}.\end{cases}$$

Also,

$$\sum_{k=0}^{p^a-1}\frac{C_k^{(2)}}{13^k}\equiv\begin{cases}1 \pmod p & \text{if } p^a\equiv\pm1,\pm5 \pmod{13},\\ 2 \pmod p & \text{if } p^a\equiv\pm2,\pm3 \pmod{13},\\ -3 \pmod p & \text{if } p^a\equiv\pm4,\pm6 \pmod{13};\end{cases}$$

and

$$\sum_{k=0}^{p^a-1}\frac{C_k^{(2)}}{19^k}\equiv\begin{cases}1 \pmod p & \text{if } p^a\equiv\pm1,\pm7,\pm8 \pmod{19},\\ -4 \pmod p & \text{if } p^a\equiv\pm2,\pm3,\pm5 \pmod{19},\\ 3 \pmod p & \text{if } p^a\equiv\pm4,\pm6,\pm9 \pmod{19}.\end{cases}$$

Now we turn to our results involving third-order and fourth-order Catalan numbers.

Theorem 1.8. *Let $p\neq5$ be a prime and let $a\in\mathbb{Z}^+$. Set*

$$S_d=\sum_{k=0}^{p^a-1}\frac{\binom{4k}{k+d}}{5^k}\quad \text{for } d=-2,-1,\ldots,3p^a.$$

(i) *When $p\neq 11$, we have*

$$S_0\equiv\begin{cases}1\pmod p&\text{if }p^a\equiv1\pmod 5,\\-9/11\pmod p&\text{if }p^a\equiv-1\pmod 5,\\-1/11\pmod p&\text{if }p^a\equiv\pm2\pmod 5;\end{cases}$$

$$S_1\equiv\begin{cases}0\pmod p&\text{if }p^a\equiv1\pmod 5,\\-5/11\pmod p&\text{if }p^a\equiv-1\pmod 5,\\-14/11\pmod p&\text{if }p^a\equiv\pm2\pmod 5;\end{cases}$$

$$S_{-1}\equiv\begin{cases}0\pmod p&\text{if }p^a\equiv1\pmod 5,\\-3/11\pmod p&\text{if }p^a\equiv-1\pmod 5,\\7/11\pmod p&\text{if }p^a\equiv2\pmod 5,\\-4/11\pmod p&\text{if }p^a\equiv-2\pmod 5;\end{cases}$$

$$S_{-2}\equiv\begin{cases}0\pmod p&\text{if }p^a\equiv1\pmod 5,\\-1/11\pmod p&\text{if }p^a\equiv-1\pmod 5,\\-16/11\pmod p&\text{if }p^a\equiv2\pmod 5,\\17/11\pmod p&\text{if }p^a\equiv-2\pmod 5.\end{cases}$$

(ii) *For $d=2,\ldots,3p^a$ we have*

$$S_d-S_{d-1}+6S_{d-2}+4S_{d-3}+S_{d-4}\equiv\begin{cases}6\pmod p&\text{if }d=p^a+1,\\4\pmod p&\text{if }d=2p^a+1,\\0\pmod p&\text{otherwise.}\end{cases}$$

(iii) *We have*

$$\sum_{k=0}^{p^a-1}\frac{C_k^{(3)}}{5^k}\equiv\begin{cases}1\pmod p&\text{if }p^a\equiv1,-2\pmod 5,\\0\pmod p&\text{if }p^a\equiv-1\pmod 5,\\-2\pmod p&\text{if }p^a\equiv2\pmod 5.\end{cases}$$

Also,

$$\sum_{k=0}^{p^a-1}\frac{\bar C_k^{(3)}}{5^k}\equiv\begin{cases}3\pmod p&\text{if }p^a\equiv1\pmod 5,\\-2\pmod p&\text{if }p^a\equiv-1\pmod 5,\\1\pmod p&\text{if }p^a\equiv\pm2\pmod 5.\end{cases}$$

Theorem 1.9. *Let $p>3$ be a prime and let $a\in\mathbb{Z}^+$. Then*

$$\sum_{k=1}^{p^a-1}\frac{3^{3k}}{4^{4k}}C_k^{(3)}\equiv\frac{(\frac{-2}{p^a})-1}{12}\pmod p$$

and

$$\sum_{k=1}^{p^a-1}\frac{3^{3k}}{4^{4k}}\binom{4k}{k+p^a}\equiv-\frac{(\frac{-2}{p^a})+20}{48}\pmod p.$$

Theorem 1.10. *Let $p > 3$ be a prime.*

(i) *If $(\frac{p}{7}) = 1$, then*

$$\sum_{k=1}^{p-1} \frac{\bar{C}_k^{(3)}}{3^k} \equiv \begin{cases} -6 \pmod p & \text{if } p \equiv 2 \pmod 3, \\ 0 \pmod p & \text{if } p = x^2 + 3y^2 \text{ and } (\frac{x+5y}{p}) = (\frac{x-3y}{p}), \\ -3 \pmod p & \text{otherwise.} \end{cases}$$

(ii) *Suppose that $(\frac{p}{23}) = 1$. In the case $p \equiv 1 \pmod 3$, if there exists an integer $t \in \mathbb{Z}$ such that $t^2 \equiv 69 \pmod p$ and $(97 - 3t)/2$ is a cubic residue modulo p then*

$$\sum_{k=1}^{p-1} (-1)^k \bar{C}_k^{(4)} \equiv 0 \pmod p,$$

otherwise

$$\sum_{k=1}^{p-1} (-1)^k \bar{C}_k^{(4)} \equiv -13 \pmod p.$$

In the case $p \equiv 2 \pmod 3$, if $v_{(p+1)/3} \equiv -13 \pmod p$ (where $v_0 = 2$, $v_1 = -97$ and $v_{n+1} = -97v_n - 13^2 v_{n-1}$ for $n \in \mathbb{Z}^+$), then

$$\sum_{k=1}^{p-1} (-1)^k \bar{C}_k^{(4)} \equiv -10 \pmod p;$$

otherwise we have

$$\sum_{k=1}^{p-1} (-1)^k \bar{C}_k^{(4)} \equiv 3 \pmod p.$$

In the next section we are going to establish a general theorem relating $\sum_{k=0}^{p^a-1} \binom{(h+1)k}{k+d} \bmod p$ to a linear recurrence of order $h + 1$. In Section 3 we shall prove Theorem 1.1. Theorems 1.2-1.6 will be proved in Section 4. (We omit the proof of Theorem 1.7 since it is similar to that of Theorem 1.6.) Section 5 is devoted to the proof of Theorem 1.8. In Section 6 we will show Theorem 1.9. The proof of Theorem 1.10 is very technical, so we omit it.

2. A general theorem

The following lemma is a well known result due to Sylvester which follows from Lagrange's interpolation formula.

Lemma 2.1. *Define an m-th linear recurrence $\{u_n\}_{n\in\mathbb{Z}}$ by*

$$u_0 = \cdots = u_{m-2} = 0, \ u_{m-1} = 1,$$

and

$$u_{n+m}+a_1u_{n+m-1}+\cdots+a_mu_n=0\quad (n\in\mathbb{Z}),$$

where $a_1,\ldots,a_m\in\mathbb{C}$ *and* $a_m\neq 0$. *Suppose that the equation* $x^m+a_1x^{m-1}+\cdots+a_0=0$ *has* m *distinct zeroes* $\alpha_1,\ldots,\alpha_n\in\mathbb{C}$. *Then*

$$u_n=\sum_{i=1}^m\frac{\alpha_i^n}{\prod_{j\neq i}(\alpha_i-\alpha_j)}\quad \text{for all } n\in\mathbb{Z}.$$

Now we present our general theorem on connections between sums involving binomial coefficients and linear recurrences.

Theorem 2.1. *Let* p *be a prime and* $m\in\mathbb{Z}_p$ *with* $m\not\equiv 0\pmod p$. *Let* $a,h\in\mathbb{Z}^+$. *Define an integer sequence* $\{u_n\}_{n\in\mathbb{Z}}$ *by*

$$u_0=\cdots=u_{h-1}=0,\ u_h=1 \tag{2.1}$$

and

$$\sum_{j=0}^{h+1}\left(\binom{h+1}{j}-m\delta_{j,h}\right)u_{n+j}=0\quad (n\in\mathbb{Z}). \tag{2.2}$$

(i) *For* $d\in\{-h+1,\ldots,hp^a\}$ *we have*

$$\begin{aligned}&\sum_{j=0}^{h+1}\left(\binom{h+1}{j}-m\delta_{j,h}\right)\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k}{k+d+j}}{m^k}\\ \equiv&[p^a\mid d+h]\binom{h+1}{(d+h)/p^a+1}\pmod p\end{aligned} \tag{2.3}$$

and

$$\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k}{k+d}}{m^k}\equiv-\sum_{r=1}^h\binom{h+1}{r+1}u_{h-1+\min\{d-rp^a,0\}}\pmod p. \tag{2.4}$$

(ii) *Suppose that*

$$D((1+x)^{h+1}-mx^h)\not\equiv 0\pmod p.$$

Then, for $d\in\{-h+1,\ldots,hp^a\}$ *we have*

$$\begin{aligned}\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k}{k+d}}{m^k}\equiv&(h+1-m)u_{d+h-1}+u_{p^a+d+h-1}\\ &+\sum_{0<r\leqslant\lfloor(d-1)/p^a\rfloor}\binom{h+1}{r+1}u_{d+h-1-rp^a}\pmod p.\end{aligned} \tag{2.5}$$

Proof. (i) We first show (2.3) for any given $d\in\{-h+1,\ldots,hp^a\}$. Observe that

$$\begin{aligned}&\frac{\binom{(h+1)p^a}{p^a+d+h}}{m^{p^a-1}}+m\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k}{k+d+h}}{m^k}\\
=&\sum_{k=1}^{p^a}\frac{\binom{(h+1)k}{k+d+h}}{m^{k-1}}=\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k+h+1}{k+d+h+1}}{m^k}\\
=&\sum_{k=0}^{p^a-1}\frac{\sum_{i=0}^{h+1}\binom{h+1}{i}\binom{(h+1)k}{k+d+h+1-i}}{m^k}\\
&\quad\text{(by the Chu-Vandermonde identity (see (5.22) of [GKP, p. 169]))}\\
=&\sum_{j=0}^{h+1}\binom{h+1}{j}\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k}{k+d+j}}{m^k}\end{aligned}$$

and hence

$$\sum_{j=0}^{h+1}\left(\binom{h+1}{j}-m\delta_{j,h}\right)\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k}{k+d+j}}{m^k}\equiv\binom{(h+1)p^a}{p^a+d+h}\ (\mathrm{mod}\ p)$$

by Fermat's little theorem. If $d+h\not\equiv 0\ (\mathrm{mod}\ p^a)$, then

$$\binom{(h+1)p^a}{p^a+d+h}=\frac{(h+1)p^a}{p^a+d+h}\binom{(h+1)p^a-1}{p^a+d+h-1}\equiv 0\ (\mathrm{mod}\ p);$$

if $d+h=p^aq$ for some $q\in\mathbb{Z}^+$, then

$$\binom{(h+1)p^a}{p^a+d+h}=\binom{(h+1)p^a}{(q+1)p^a}\equiv\binom{h+1}{q+1}\ (\mathrm{mod}\ p)$$

by Lucas' theorem (see, e.g., [HS]). Therefore (2.3) follows from the above.

Next we want to prove (2.4) by induction.

For $d\in\{hp^a-h,\ldots,hp^a\}$, as $d\geqslant h(p^a-1)$ and $(h-1)p^a-d\leqslant h-p^a<h$ we have

$$\sum_{k=0}^{p^a-1}\frac{\binom{(h+1)k}{k+d}}{m^k}=\frac{\binom{(h+1)(p^a-1)}{p^a-1+d}}{m^{p^a-1}}\equiv\delta_{d,h(p^a-1)}\ (\mathrm{mod}\ p)$$

and also

$$\begin{aligned}&\sum_{i=1}^{h}\binom{h+1}{i+1}u_{h-1+\min\{d-ip^a,0\}}\\
=&\sum_{\substack{1\leqslant i\leqslant h\\ ip^a\geqslant d+h}}\binom{h+1}{i+1}u_{h-1+d-ip^a}\\
=&[hp^a\geqslant d+h]u_{h-1+d-hp^a}=\delta_{d,hp^a-h}u_{-1}=-\delta_{d,h(p^a-1)}.\end{aligned}$$

So (2.4) holds for all $d = hp^a - h, \ldots, hp^a$.

Let $-h < d < hp^a - h$ and assume that (2.4) with d replaced by a large integer not exceeding hp^a holds. For $r \in \{1, \ldots, h\}$, if $ip^a < d + h$ then

$$\sum_{j=0}^{h+1}\left(\binom{h+1}{j} - m\delta_{j,h}\right)u_{h-1+\min\{d+j-rp^a,0\}} = 0$$

since $u_0 = \cdots = u_{h-1} = 0$; if $ip^a \geqslant d + h$, then

$$\begin{aligned}&\sum_{j=0}^{h+1}\left(\binom{h+1}{j} - m\delta_{j,h}\right)u_{h-1+\min\{d+j-rp^a,0\}}\\ =&\sum_{j=0}^{h}\left(\binom{h+1}{j} - m\delta_{j,h}\right)u_{h-1+d+j-rp^a} + u_{h-1+\min\{d+h+1-rp^a,0\}}\\ =&\sum_{j=0}^{h}\left(\binom{h+1}{j} - m\delta_{j,h}\right)u_{h-1+d+j-rp^a} - \delta_{d+h,rp^a} = -\delta_{d+h,rp^a}.\end{aligned}$$

So we have

$$\begin{aligned}&\sum_{j=0}^{h+1}\left(\binom{h+1}{j} - m\delta_{j,h}\right)\sum_{r=1}^{h}\binom{h+1}{r+1}u_{h-1+\min\{d+j-rp^a,0\}}\\ =&\sum_{i=1}^{h}\binom{h+1}{r+1}\sum_{j=0}^{h+1}\left(\binom{h+1}{j} - m\delta_{j,h}\right)u_{h-1+\min\{d+j-rp^a,0\}}\\ =&\sum_{r=1}^{h}\binom{h+1}{r+1}(-\delta_{rp^a,d+h}) = -[p^a \mid d+h]\binom{h+1}{(d+h)/p^a+1}.\end{aligned}$$

Combining this with (2.3) and the induction hypothesis, we obtain (2.4). This concludes the induction step.

(ii) Write

$$\sum_{j=0}^{h+1}\left(\binom{h+1}{j} - m\delta_{j,h}\right)x^j = (x+1)^{h+1} - mx^h = \prod_{i=1}^{h+1}(x - \alpha_i)$$

with $\alpha_1, \ldots, \alpha_{h+1} \in \mathbb{C}$. As $D := D((x+1)^{h+1} - mx^h) \neq 0$, $\alpha_1, \ldots, \alpha_{h+1}$ are distinct. Clearly all those α_i, α_i^{-1}, and

$$c_i := \frac{D}{\prod_{j\neq i}(\alpha_i - \alpha_j)} = \prod_{\substack{1\leqslant s<t\leqslant h+1\\ s,t\neq i}}(\alpha_s - \alpha_t)^2 \times \prod_{j\neq i}(\alpha_i - \alpha_j)$$

are algebraic integers.

Fix $d \in \{-h+1, \ldots, dp^a\}$. By part (i),

$$-\sum_{k=0}^{p^a-1} \frac{\binom{(h+1)k}{k+d}}{m^k} \equiv \sum_{\substack{1 \leqslant r \leqslant h \\ rp^a \geqslant d}} \binom{h+1}{r+1} u_{h-1+d-rp^a} \pmod p.$$

By Lemma 2.1, for any $n \in \mathbb{N}$ we have

$$u_n = \sum_{i=1}^{h+1} \frac{\alpha_i^n}{\prod_{j \neq i}(\alpha_i - \alpha_j)} = \frac{1}{D} \sum_{i=1}^{h+1} c_i \alpha_i^n.$$

Therefore

$$-\sum_{k=0}^{p^a-1} \frac{\binom{(h+1)k}{k+d}}{m^k} \equiv \frac{1}{D} \sum_{i=1}^{h+1} c_i \alpha_i^{d+h-1} \sum_{\substack{1 \leqslant r \leqslant h \\ rp^a \geqslant d}} \binom{h+1}{r+1} \alpha_i^{-rp^a} \pmod p.$$

Since

$$\sum_{j=0}^{h+1} \binom{h+1}{j} \alpha_i^{jp^a} \equiv \left(\sum_{j=0}^{h+1} \binom{h+1}{j} \alpha_i^j \right)^{p^a} = (m\alpha_i^h)^{p^a} \equiv m\alpha_i^{hp^a} \pmod p,$$

we have

$$m \equiv \sum_{j=0}^{h+1} \binom{h+1}{j} \alpha_i^{(j-h)p^a} = \sum_{r=-1}^{h} \binom{h+1}{r+1} \alpha_i^{-rp^a} \pmod p$$

and hence

$$\sum_{r=1}^{h} \binom{h+1}{r+1} \alpha_i^{-rp^a} \equiv m - h - 1 - \alpha_i^{p^a} \pmod p.$$

Therefore $\sum_{k=0}^{p^a-1} \binom{(h+1)k}{k+d}/m^k$ is congruent to

$$\begin{aligned} &\frac{1}{D} \sum_{i=1}^{h+1} c_i \alpha_i^{d+h-1} \Bigg(h + 1 - m + \alpha_i^{p^a} + \sum_{0 < rp^a \leqslant d-1} \binom{h+1}{r+1} \alpha_i^{-rp^a} \Bigg) \\ =&(h+1-m)u_{d+h-1} + u_{p^a+d+h-1} + \sum_{0 < r \leqslant \lfloor (d-1)/p^a \rfloor} \binom{h+1}{r+1} u_{d+h-1-rp^a} \end{aligned}$$

modulo p. This proves (2.5).

The proof of Theorem 2.1 is now complete. $\square$

3. Proof of Theorem 1.1

To prove Theorem 1.1 in the case $c \equiv -1/4 \pmod p$, we give the following theorem.

Theorem 3.1. *Let $p > 3$ be a prime and let $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1} \frac{4^k}{27^k}\binom{3k}{k+d} \equiv \begin{cases} ((-1)^d 4^{2-d} - 7(9d+1)2^d)/81 \pmod p & \text{if } d \in \{-1,\ldots,p^a\}, \\ ((-1)^d 4^{3-d} - (9d+1)2^d)/81 \pmod p & \text{if } d \in \{p^a,\ldots,2p^a\}. \end{cases} \tag{3.1}$$

In particular,

$$\sum_{k=0}^{p^a-1} \frac{4^k}{27^k}\binom{3k}{k} \equiv \frac{1}{9} \pmod p, \quad \sum_{k=1}^{p^a-1} \frac{4^k}{27^k}\binom{3k}{k+p^a} \equiv -\frac{2}{9} \pmod p,$$

$$\sum_{k=1}^{p^a-1} \frac{4^k}{27^k}\binom{3k}{k+1} \equiv -\frac{16}{9} \pmod p, \quad \sum_{k=1}^{p^a-1} \frac{4^k}{27^k}\binom{3k}{k-1} \equiv -\frac{4}{9} \pmod p.$$

Proof. Let $u_0 = u_1 = 0,\ u_2 = 1$, and

$$u_{n+3} + \left(3 - \frac{27}{4}\right)u_{n+1} + u_n = 0 \quad \text{for } n = 0,1,2,\ldots.$$

Since

$$x^3 + \left(3 - \frac{27}{4}\right)x^2 + 3x + 1 = \left(x + \frac{1}{4}\right)(x-2)^2,$$

there are $a,b,c \in \mathbb{C}$ such that $u_n = (an+b)2^n + c(-1/4)^n$ for all $n \in \mathbb{N}$. By $u_0 = u_1 = 0$ and $u_2 = 1$, we can easily determine the values of a,b,c explicitly. It follows that

$$u_n = \frac{16}{81}\left(\left(-\frac{1}{4}\right)^n + \left(\frac{9}{8}n - 1\right)2^n\right) \quad \text{for all } n \in \mathbb{N}. \tag{3.2}$$

Let $d \in \{-1,\ldots,2p^a\}$. Applying (2.4) with $h = 2$ and $m = 27/4$ we get

$$-\sum_{k=0}^{p^a-1} \frac{4^k}{27^k}\binom{3k}{k+d} \equiv \sum_{r=1}^{2}\binom{3}{r+1}u_{1+\min\{d-rp^a,0\}}$$
$$\equiv 3[d \leqslant p^a]u_{1+d-p^a} + u_{1+d-2p^a} \pmod p.$$

By (3.2) and Fermat's little theorem,

$$u_{d+1-p^a} \equiv \frac{(-1)^d 4^{2-d} + (9d+1)2^{d+1}}{81} \pmod p$$

and

$$u_{d+1-2p^a} \equiv \frac{(-1)^{d-1} 4^{3-d} + (9d+1)2^{d}}{81} \pmod p.$$

Thus (3.1) follows.

Applying (3.1) with $d = 0, \pm 1, p^a$ we immediately obtain the last four congruences in Theorem 3.1. We are done. □

Now we need some knowledge about Lucas sequences.

Given $A, B \in \mathbb{C}$ with $B \neq 0$, the Lucas sequences $u_n = u_n(A,B)$ and $v_n = v_n(A,B)$ $(n \in \mathbb{Z})$ are defined as follows:

$$\begin{aligned} &u_0 = 0,\ u_1 = 1,\ \text{and } u_{n+1} = Au_n - Bu_{n-1}\ (n \in \mathbb{Z}); \\ &v_0 = 2,\ v_1 = A,\ \text{and } v_{n+1} = Av_n - Bv_{n-1}\ (n \in \mathbb{Z}). \end{aligned}$$

It ie easy to see that $v_n = 2u_{n+1} - Au_n$ for all $n \in \mathbb{Z}$. Let α and β be the two roots of the equation $x^2 - Ax + B = 0$. It is well known that

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

Lemma 3.1. *Let p be an odd prime and let $a \in \mathbb{Z}^+$. Let $A, B \in \mathbb{Z}_p$ with $\Delta = A^2 - 4B \not\equiv 0 \pmod p$. Then for any $n \in \mathbb{Z}$ we have*

$$u_{n+p^a} \equiv \frac{Au_n + (\frac{\Delta}{p^a})v_n}{2} \pmod p \text{ and } Bu_{n-p^a} \equiv \frac{Au_n - (\frac{\Delta}{p^a})v_n}{2} \pmod p,$$

where $u_k = u_k(A,B)$ and $v_k = v_k(A,B)$.

Proof. Let α and β be the two roots of the equation $x^2 - Ax + B = 0$. Clearly

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

Since

$$(\alpha - \beta)u_{p^a} = \alpha^{p^a} - \beta^{p^a} \equiv (\alpha - \beta)^{p^a} \pmod p,$$

we have

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

and hence

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

Now,

$$\begin{aligned}2u_{n+p^a} =&\frac{\alpha^n-\beta^n}{\alpha-\beta}(\alpha^{p^a}+\beta^{p^a})+\frac{\alpha^{p^a}-\beta^{p^a}}{\alpha-\beta}(\alpha^n+\beta^n)\\ =&u_nv_{p^a}+u_{p^a}v_n\equiv Au_n+\left(\frac{\Delta}{p}\right)v_n \pmod p.\end{aligned}$$

Also,

$$\begin{aligned}2u_{n-p^a} =&\frac{\alpha^n-\beta^n}{\alpha-\beta}(\alpha^{-p^a}+\beta^{-p^a})+\frac{\alpha^{-p^a}-\beta^{-p^a}}{\alpha-\beta}(\alpha^n+\beta^n)\\ =&u_n\frac{\alpha^{p^a}+\beta^{p^a}}{(\alpha\beta)^{p^a}}+\frac{\beta^{p^a}-\alpha^{p^a}}{\alpha-\beta}\cdot\frac{v_n}{(\alpha\beta)^{p^a}}=u_n\frac{v_{p^a}}{B^{p^a}}-\frac{u_{p^a}}{B^{p^a}}v_n\end{aligned}$$

and hence

$$2Bu_{n-p^a}\equiv 2B^{p^a}u_{n-p^a}=u_nv_{p^a}-u_{p^a}v_n\equiv Au_n-\left(\frac{\Delta}{p^a}\right)v_n \pmod p.$$

This concludes the proof. $\square$

For Theorem 1.1 in the case $c\not\equiv -1/4 \pmod p$, we need the following general result.

Theorem 3.2. *Let p be an odd prime and let $a\in\mathbb{Z}^+$. Let $c\in\mathbb{Z}_p$ with $c\not\equiv 0,-1,2,-1/4 \pmod p$, and let $d\in\{-1,0,\ldots,p^a\}$. Then*

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\frac{c^{2k}}{(c+1)^{3k}}\binom{3k}{k+d}\\ \equiv&u_{d+1}+\frac{3c+1}{(c+1)^2(c-2)}\left(u_{d+1}-c^d+\frac{u_d}{c^2}\right)\\ &+\frac{v_d+c^2v_{d+1}}{2(c+1)^2(c-2)}\left(1-\left(\frac{4c+1}{p^a}\right)\right) \pmod p,\end{aligned}\tag{3.3}$$

where $u_n=u_n((3c+1)/c^2,-1/c)$ and $v_n=v_n((3c+1)/c^2,-1/c)$.

Proof. Set $m=(c+1)^3/c^2$. Then c is a zero of the polynomial

$$x^2+(3-m)x^2+3x+1=(x+1)^3-mx^2.$$

The discriminant of this polynomial is $D=(4m-27)m^2$. Note that

$$c^2(4m-27)=4(c+1)^3-27c^2=(4c+1)(c-2)^2\not\equiv 0 \pmod p.$$

We can write

$$x^2+(3-m)x^2+3x+1=(x-c)(x-\alpha)(x-\beta)$$

with α,β,c distinct. Clearly $-c-\alpha-\beta=3-m$ and $(-c)(-\alpha)(-\beta)=1$. It follows that $\alpha+\beta=A$ and $\alpha\beta=B$, where $A=(3c+1)/c^2$ and $B=-1/c$.

Let $U_0=U_1=0$, $U_2=1$ and $U_{n+3}+(3-m)U_{n+2}+3U_{n+1}+U_n=0$ for $n\in\mathbb{Z}$. Also set $u_n=u_n(A,B)$ and $v_n=v_n(A,B)$ for $n\in\mathbb{Z}$. By Lemma 2.1, for any $n\in\mathbb{Z}$ we have

$$\begin{aligned}U_n=&\frac{c^n}{(c-\alpha)(c-\beta)}+\frac{\alpha^n}{(\alpha-c)(\alpha-\beta)}+\frac{\beta^n}{(\beta-c)(\beta-\alpha)}\\ =&\frac{1}{(c-\alpha)(c-\beta)}\left(c^n+\frac{\alpha^n(\beta-c)-(\alpha-c)\beta^n}{\alpha-\beta}\right)\\ =&\frac{1}{c^2-Ac+B}\left(c^n+B\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}-c\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)\\ =&\frac{c}{c^3-3c-2}(c^n-c^{-1}u_{n-1}-cu_n)=\frac{c^{n+1}-u_{n-1}-c^2u_n}{(c+1)^2(c-2)}.\end{aligned}$$

In light of Theorem 2.1(ii),

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k+d}}{m^k}\equiv(3-m)U_{d+1}+U_{p^a+d+1}\pmod p$$

and hence

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\frac{c^{2k}}{(c+1)^{3k}}\binom{3k}{k+d}-U_{p^a+d+1}\\ \equiv&\left(3-\frac{(c+1)^3}{c^2}\right)\frac{c^{d+2}-u_d-c^2u_{d+1}}{(c+1)^2(c-2)}\pmod p).\end{aligned}\tag{3.4}$$

Note that

$$\Delta:=A^2-4B=\frac{(3c+1)^2}{c^4}+\frac{4}{c}=\frac{(c+1)^2(4c+1)}{c^4}\not\equiv0\pmod p$$

and

$$\left(\frac{\Delta}{p^a}\right)=\left(\frac{4c+1}{p^a}\right).$$

By Lemma 3.1,

$$2u_{p^a+d}\equiv\left(\frac{4c+1}{p}\right)v_d+Au_d\pmod p$$

and

$$2u_{p^a+d+1} \equiv \left(\frac{4c+1}{p}\right) v_{d+1} + Au_{d+1} \pmod p.$$

Thus

$$\begin{aligned} U_{p^a+d+1} =& \frac{c^{p^a+d+2} - u_{p^a+d} - c^2 u_{p^a+d+1}}{(c+1)^2(c-2)} \\ \equiv& \frac{2c^{d+3} - ((\frac{4c+1}{p})v_d + Au_d) - c^2((\frac{4c+1}{p})v_{d+1} + Au_{d+1})}{2(c+1)^2(c-2)} \pmod p. \end{aligned}$$

Note that

$$\begin{aligned} &\frac{v_d + c^2 v_{d+1}}{2} + A\frac{u_d + c^2 u_{d+1}}{2} \\ =&\frac{v_d + Au_d}{2} + c^2\frac{v_{d+1} + Au_{d+1}}{2} = u_{d+1} + c^u_{d+2} \\ =&u_{d+1} + c^2\left(\frac{3c+1}{c^2}u_{d+1} + \frac{u_d}{c}\right) = (3c+2)u_{d+1} + cu_d. \end{aligned}$$

Therefore

$$U_{p^a+d+1} \equiv \frac{c^{d+3} + (v_d + c^2 v_{d+1})\frac{1-(\frac{4c+1}{p^a})}{2} - ((3c+2)u_{d+1} + cu_d)}{(c+1)^2(c-2)} \pmod p.$$

Combining this with (3.4) we finally obtain the desired (3.3). □

Corollary 3.1. *Let $p > 3$ be a prime and let $d \in \{-1, 0, \dots, p^a\}$ with $a \in \mathbb{Z}^+$. Then*

$$\sum_{k=0}^{p^a-1} \frac{3^k}{8^k}\binom{3k}{k+d} \equiv \begin{cases} \frac{(-3)^{d/2}}{28}(1 + 27(\frac{p^a}{3})) \pmod p, & \text{if } 2 \mid d, \\ \frac{(-3)^{(d+3)/2}}{28}(1 - (\frac{p^a}{3})) \pmod p, & \text{if } 2 \nmid d. \end{cases} \tag{3.5}$$

Proof. Set $c = -1/3$. Then $c^2/(c+1)^3 = 3/8$, $(3c+1)/c^2 = 0$ and $-1/c = 3$. Let $u_n = u_n(0,3)$ and $v_n = v_n(0,3)$ for $n \in \mathbb{Z}$. We clearly have

$$u_{2n} = v_{2n+1} = 0,\ u_{2n+1} = (-3)^n \text{ and } v_{2n} = 2(-3)^n \quad \text{for all } n \in \mathbb{Z}.$$

Applying Theorem 3.2 we immediately get the desired result. □

Proof of Theorem 1.1. In the case $c \equiv -1/4 \pmod p$, we have $c^2/(c+1)^3 \equiv 4/27 \pmod p$ and $c' \equiv -8/9 \pmod p$, hence the desired congruences follow from Theorem 3.1.

Below we assume that $c \not\equiv -1/4 \pmod p$. For the first three congruences in Theorem 1.1, we may simply apply Theorem 3.2 with $d = 0, \pm 1$.

As in the proof of Theorem 3.2, we define $A = (3c+1)/c^2$, $B = -1/c$ and $\Delta = A^2 - 4B$. Let $u_n = u_n(A, B)$ and $v_n = v_n(A, B)$ for $n \in \mathbb{Z}$. By Lemma 3.1,

$$2u_{p^a+1} = Au_1 + \left(\frac{\Delta}{p^a}\right) v_1 = A + A\left(\frac{4c+1}{p^a}\right) \pmod p$$

and

$$\begin{aligned} v_{p^a+1} =& 2u_{p^a+2} - Au_{p^a+1} = Au_{p^a+1} - 2Bu_{p^a} \\ \equiv& \frac{A^2 + A^2(\frac{4c+1}{p^a})}{2} - 2B\left(\frac{4c+1}{p^a}\right) = \frac{A^2 + \Delta(\frac{4c+1}{p^a})}{2} \pmod p. \end{aligned}$$

These, together with Theorem 3.2 in the case $d = p^a$, yield the last congruence in Theorem 1.1. We are done. □

4. Proofs of Theorems 1.2-1.6

Lemma 4.1. *Let $p > 3$ be a prime and let $a \in \mathbb{Z}^+$. Let*

$$u_0 = u_1 = 0,\ u_2 = 1,\ \text{and}\ u_{n+3} + a_1u_{n+2} + a_2u_{n+1} + a_3u_n = 0\ \text{for all}\ n \in \mathbb{N},$$

where $a_1, a_2, a_3 \in \mathbb{Z}$. Suppose that $d \in \mathbb{Z}$ and

$$d^2 \equiv D(x^3 + a_1x^2 + a_2x + a_3) \not\equiv 0 \pmod p.$$

Set $b = -2a_1^3 + 9a_1a_2 - 27a_3$. Then

$$u_{p^a} \equiv \begin{cases} 0 \pmod p & \text{if } p \mid a_1^2 - 3a_2 \text{ or } b/(3d) \in C_0(p^a), \\ \pm(a_1^2 - 3a_2)/d \pmod p & \text{if } \pm b/(3d) \in C_1(p^a); \end{cases}$$

$$u_{p^a+1} \equiv \begin{cases} b^{(p^a-1)/3} \pmod p & \text{if } p \mid a_1^2 - 3a_2, \\ 1 \pmod p & \text{if } b/(3d) \in C_0(p^a), \\ (\pm(9a_3 - a_1a_2) - d)/(2d) \pmod p & \text{if } \pm b/(3d) \in C_1(p^a); \end{cases}$$

$$u_{p^a+2} \equiv \begin{cases} -a_1(2b^{(p^a-1)/3} + 1)/3 \pmod p & \text{if } p \mid a_1^2 - 3a_2, \\ -a_1 \pmod p & \text{if } b/(3d) \in C_0(p^a), \\ \pm(a_2^2 - 3a_1a_3)/d \pmod p & \text{if } \pm b/(3d) \in C_1(p^a). \end{cases}$$

Proof. In the case $a = 1$, this is a result due to Z. H. Sun [S03, Theorems 3.2-3.3]. Modifying the proof for the case $a = 1$ slightly, we get the result with general a. □

Actually we just need the following particular result implied by Lemma 4.1.

Lemma 4.2. *Let $p>3$ be a prime and let $a\in\mathbb{Z}^+$. Let $m,t\in\mathbb{Z}$ with $2t+1\not\equiv 0 \pmod p$ $m\equiv t^2+t+7\not\equiv 0 \pmod p$. Define $\{u_n\}_{n\geqslant 0}$ by*

$$u_0=u_1=0,\ u_2=1,\ \text{and } u_{n+3}+(3-m)u_{n+2}+3u_{n+1}+u_n=0 \text{ for } n\in\mathbb{N}.$$

Set $c=(2m^2-18m+27)/(6t+3)$. Then

$$u_{p^a}\equiv\begin{cases}0 \pmod p & \text{if } p\mid m-6 \text{ or } c\in C_0(p^a),\\ \pm(m-6)/(2t+1) \pmod p & \text{if } \pm c\in C_1(p^a);\end{cases}$$

$$u_{p^a+1}\equiv\begin{cases}2^{(p^a-1)/3} \pmod p & \text{if } p\mid m-6,\\ 1 \pmod p & \text{if } c\in C_0(p^a),\\ \pm 3/(4t+2)-1/2 \pmod p & \text{if } \pm c\in C_1(p^a);\end{cases}$$

$$u_{p^a+2}\equiv\begin{cases}2^{(p^a+2)/3}+1 \pmod p & \text{if } p\mid m-6,\\ m-3 \pmod p & \text{if } c\in C_0(p^a),\\ \pm 3/(2t+1) \pmod p & \text{if } \pm c\in C_1(p^a).\end{cases}$$

Proof of Theorem 1.2. The discriminant of the polynomial $(x+1)^3-6x^2$ is $D=(4\times 6-27)6^2=-108$.

Case 1. $p\equiv -1 \pmod 3$. In this case, $(\frac{D}{p})=-1$ and hence $(x+1)^2-6x^2$ mod p has exactly two irreducible factors, thus $(c+1)^3\equiv 6c^2 \pmod p$ for some $c\in\mathbb{Z}$. Clearly $c\not\equiv 0,-1,2,-1/4 \pmod p$. Note that a is even since $p^a\equiv 1 \pmod 3$. As

$$\left(\frac{4c+1}{p^a}\right)=\left(\frac{4c+1}{p}\right)^a=1,$$

the first congruence in Theorem 1.2 follows from Theorem 1.1.

Case 2. $p\equiv 1 \pmod 3$. In this case, for some $t\in\mathbb{Z}$ we have $(2t+1)^2\equiv -3 \pmod p$, i.e., $t^2+t+7\equiv 6 \pmod p$. Let $u_0=u_1=0$, $u_2=1$ and

$$u_{n+3}+(3-6)u_{n+2}+3u_{n+1}+u_n=0\ (n=0,1,2,\ldots).$$

By Theorem 2.1(ii), for $d=-1,\ldots,p^a$ we have

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k+d}}{6^k}\equiv u_{p^a+d+1}+(3-6)u_{d+1} \pmod p.$$

Combining this with Lemma 4.2 in the case $m=6$, we are able to determine $\sum_{k=0}^{p^a-1}\binom{3k}{k+d}/6^k$ mod p for $d=0,\pm1$. Note that

$$\bar{C}_k^{(2)}=\frac{2}{k+1}\binom{3k}{k}=2\binom{3k}{k}-\binom{3k}{k+1}.$$

So we have all the desired congruences in Theorem 1.2. $\square$

Proof of Theorem 1.3. Define $\{u_n\}_{n\geqslant 0}$ as in Lemma 4.2. By Theorem 2.1(ii), for $d=-1,\ldots,p^a$ we have

$$\sum_{k=0}^{p^a-1}\frac{\binom{3k}{k+d}}{m^k}\equiv u_{p^a+d+1}+(3-m)u_{d+1}\ (\mathrm{mod}\ p).$$

Observe that $c^2+3\not\equiv 0\ (\mathrm{mod}\ p)$ since

$$(2m^2-18m+27)^2+3(6t+3)^2\equiv 4m(m-6)^2\ (\mathrm{mod}\ p).$$

By applying Lemma 4.2 we obtain the desired result. $\square$

Proof of Theorem 1.4. Fix $d\in\{0,\pm1\}$. By Theorem 3.1 (or Theorem 1.1 in the case $c=-1/4$),

$$\sum_{k=1}^{p^a-1}\frac{4^k}{27^k}\binom{3k}{k+d}\equiv-\frac{2^{d+3}}{9}\ (\mathrm{mod}\ p).$$

Let $m\in\{1,\ldots,p-1\}$ with $m\not\equiv 27/4\ (\mathrm{mod}\ p)$. If $(c+1)^3\equiv mc^2\ (\mathrm{mod}\ p)$ for some $c\in\mathbb{Z}$, then $c\not\equiv 0,-1,2,-1/4\ (\mathrm{mod}\ p)$. Thus, by Theorem 1.1 we have

$$\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k+d}}{m^k}\equiv 0\ (\mathrm{mod}\ p)$$

since $(\frac{4c+1}{p^a})=(\frac{4c+1}{p})^a=1$.

Now assume that $(x+1)^3\equiv 6x^2\ (\mathrm{mod}\ p)$ is not solvable over $\mathbb{Z}$. Then, by Stickelberger's theorem,

$$\left(\frac{p}{3}\right)=\left(\frac{-108}{p}\right)=\left(\frac{D((1+x)^3-3x^2)}{p}\right)\equiv(-1)^3-1=1$$

and hence $p\equiv 1\ (\mathrm{mod}\ 3)$. By Theorem 1.2,

$$\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k+d}}{6^k}\equiv 0\ (\mathrm{mod}\ p)$$

since

$$2^{(p^6-1)/3}=2^{(p^2-1)(p^4+p^2+1)/3}\equiv 1\ (\mathrm{mod}\ p).$$

Now suppose that $m\not\equiv 6\pmod p$ and $(x+1)^3\equiv mx^2\pmod p$ is not solvable over $\mathbb{Z}$. Then

$$\left(\frac{(4m-27)m^2}{p}\right)=\left(\frac{D((x+1)^3-mx^2)}{p}\right)=1$$

and hence $m\equiv t^2+t+7\pmod p$ for some $t\in\mathbb{Z}$ with $t\not\equiv -1/2\pmod p$. Let $c=(2m^2-18m+27)/(6t+3)$. By Theorem 1.3,

$$\left(\frac{c+1+2\omega}{p^a}\right)_3=\left(\frac{c+1+2\omega}{p}\right)_3^3=1.$$

Hence $c\in C_0(p^a)$ and

$$\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k+d}}{m^k}\equiv 0\pmod p.$$

In view of the above,

$$\begin{aligned}-\sum_{\substack{0<k<p^a\\ k\equiv r\ (\mathrm{mod}\ p-1)}}\binom{3k}{k+d}&\equiv\sum_{k=1}^{p^a-1}\binom{3k}{k+d}(p-1)[p-1\mid k-r]\\ &\equiv\sum_{k=1}^{p^a-1}\binom{3k}{k+d}\sum_{m=1}^{p-1}m^{r-k}=\sum_{m=1}^{p-1}m^r\sum_{k=1}^{p^a-1}\frac{\binom{3k}{k+d}}{m^k}\\ &\equiv\frac{27^r}{4^r}\sum_{k=1}^{p^a-1}\frac{4^k}{27^k}\binom{3k}{k+d}\equiv-\frac{27^r}{4^r}\cdot\frac{2^{d+3}}{9}\pmod p.\end{aligned}$$

So we have the first congruence in Theorem 1.4. The second congruence follows immediately since

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

and

$$\sum_{r=0}^{p-2}\frac{27^r}{4^r}=\frac{27^{p-1}/4^{p-1}-1}{27/4-1}\equiv-[p=23]\pmod p.$$

This concludes the proof of Theorem 1.4. $\square$

Proof of Theorem 1.5. It suffices to deduce the first, the second and the third congruences in Theorem 1.5. Since we can handle the case $p=2$ by detailed analysis, below we assume $p>3$.

By Theorem 1.3 in the case $m=9$ and $t=1$, we only need to show that

$$\begin{aligned}
3\in C_0(p^a) &\iff p^a\equiv\pm1 \pmod 9,\\
3\in C_1(p^a) &\iff p^a\equiv\pm2 \pmod 9,\\
3\in C_2(p^a) &\iff p^a\equiv\pm4 \pmod 9.
\end{aligned}\tag{4.1}$$

Note that

$$\left(\frac{3+1+2\omega}{p^a}\right)_3=\left(\frac{2}{p}\right)_3^a\left(\frac{2+\omega}{p^a}\right)_3=\left(\frac{2+\omega}{p^a}\right)$$

and

$$\overline{\left(\frac{2+\omega}{p^a}\right)_3}=\left(\frac{2+\bar\omega}{p^a}\right)_3=\left(\frac{1-\omega}{p^a}\right)_3=\omega^{((\frac{p^a}{3})p^a-1)/3}.$$

(See, e.g., [IR].) Clearly,

$$\frac{(\frac{p^a}{3})p^a-1}{3}\equiv\begin{cases}0 & \text{if } p^a\equiv\pm1 \pmod 9,\\ 2 \pmod 3 & \text{if } p^a\equiv\pm2 \pmod 9,\\ 1 \pmod 3 & \text{if } p^a\equiv\pm4 \pmod 9.\end{cases}$$

Therefore the three formulae in (4.1) are valid. We are done. □

Proof of Theorem 1.6. We only need to deduce the first, the second and the third congruences in Theorem 1.6. Since we can handle the case $p=2,3$ by detailed analysis, below we assume $p>3$.

By Theorem 1.3 in the case $m=7$ and $t=0$, it suffices to show that

$$\begin{aligned}
-\frac13\in C_0(p^a) &\iff p^a\equiv\pm1 \pmod 7,\\
-\frac13\in C_1(p^a) &\iff p^a\equiv\pm3 \pmod 7,\\
-\frac13\in C_2(p^a) &\iff p^a\equiv\pm2 \pmod 7.
\end{aligned}\tag{4.2}$$

Clearly

$$\left(\frac{3}{p^a}\right)_3\left(\frac{-1/3+1+2\omega}{p^a}\right)_3=\left(\frac{2}{p^a}\right)_3\left(\frac{1+3\omega}{p^a}\right)_3,$$

and hence

$$\left(\frac{-1/3+1+2\omega}{p^a}\right)_3=\left(\frac{1+3\omega}{p^a}\right)_3$$

since $(\frac{2}{p^a})=(\frac{3}{p^a})=1$. Observe that the norm of $1+3\omega$ is $N(1+3\omega)=(1+3\omega)(1+3\bar\omega)=7$. By the cubic reciprocity law,

$$\left(\frac{1+3\omega}{p^a}\right)_3=\left(\frac{p^a}{1+3\omega}\right)_3.$$

If $p^a \equiv \pm 1 \pmod 7$, then

$$\left(\frac{p^a}{1+3\omega}\right)_3 = \left(\frac{\pm 1}{1+3\omega}\right)_3 = \left(\frac{\pm 1}{1+3\omega}\right)_3^3 = 1$$

and hence $-1/3 \in C_0(p^a)$. If $p^a \equiv \pm 2 \pmod 7$, then

$$\left(\frac{p^a}{1+3\omega}\right)_3 = \left(\frac{\pm 2}{1+3\omega}\right)_3 \equiv (\pm 2)^{(N(1+3\omega)-1)/3} = 4 \equiv \omega^2 \pmod{1+3\omega},$$

hence $(\frac{p^a}{1+3\omega})_3 = \omega^2$ and $-1/3 \in C_2(p^a)$. If $p^a \equiv \pm 4 \pmod 7$, then

$$\left(\frac{p^a}{1+3\omega}\right)_3 = \left(\frac{\pm 4}{1+3\omega}\right)_3 = \left(\frac{2}{1+3\omega}\right)_3^2 = (\omega^2)^2 = \omega$$

and hence $-1/3 \in C_1(p^a)$. This completes the proof. □

5. Proof of Theorem 1.8

In this section we define a sequence $\{u_n\}_{n\in\mathbb{Z}}$ by

$$u_0 = u_1 = u_2 = 0,\ u_3 = 1$$

and

$$u_{n+4} - u_{n+3} + 6u_{n+2} + 4u_{n+1} + u_n = 0 \quad (n \in \mathbb{Z}).$$

We also set

$$v_n^{(1)} = u_{n+2} - 3u_{n+1} \quad \text{and} \quad v_n^{(2)} = 3u_{n+1} + 2u_n. \tag{5.1}$$

Recall that the Lucas sequence $\{L_n\}_{n\in\mathbb{Z}}$ is given by

$$L_0 = 2,\ L_1 = 1, \text{and } L_{n+1} = L_n + L_{n-1} \quad \text{for all } n \in \mathbb{Z}.$$

Lemma 5.1. (i) *We have*

$$x^4 - x^3 + 6x^2 + 4x + 1 = (x+1)^4 - 5x^3 = \prod_{\substack{\zeta^5=1\\ \zeta\neq 1}} (x - (1+\zeta)^2). \tag{5.2}$$

(ii) *Let p be a prime, and let $a \in \mathbb{Z}^+$ and $s \in \{1,2\}$. Then, for any $d \in \mathbb{N}$ we have*

$$\begin{aligned}5(v_{p^a+d}^{(s)} - v_d^{(s)}) \equiv\, & 2L_{2d}([5 \mid d+2p^a-2s+1] - [5 \mid d+2p^a-2s])\\
&+ 4L_{2d}([5 \mid d+p^a-2s+1] - [5 \mid d+p^a-2s])\\
&+ \left(\frac{d+2p^a-2s+1}{5}\right) L_{2d-(\frac{d+2p^a-2s+1}{5})}\\
&- \left(\frac{d+2p^a-2s}{5}\right) L_{2d-(\frac{d+2p^a-2s}{5})}\\
&+ 2\left(\frac{d+p^a-2s+1}{5}\right) L_{2d-(\frac{d+p^a-2s+1}{5})}\\
&- 2\left(\frac{d+p^a-2s}{5}\right) L_{2d-(\frac{d+p^a-2s}{5})} \pmod p.\end{aligned}$$

Proof. (i) It is easy to verify that

$$(1+(1+x)^2)^4-5(1+x)^6=\frac{x^5-1}{x-1}(x^4+7x^3+19x^2+23x+11).$$

Therefore any primitive 5th root ζ of unity is a zero of $(1+x)^4=5x^3$. So (5.2) follows.

(ii) For $n\in\mathbb{Z}$ let

$$V_n^{(s)}=\frac{1}{5}\sum_{\substack{\zeta^5=1\\ \zeta\neq1}}(\zeta^{1-2s}-\zeta^{-2s})(1+\zeta)^{2n}=\frac{1}{5}\sum_{\zeta^5=1}(\zeta^{1-2s}-\zeta^{-2s})(1+\zeta)^{2n}.$$

Then $\{V_n\}_{n\in\mathbb{Z}}$ satisfies the recurrence relation

$$V_{n+4}^{(s)}-V_{n+3}^{(s)}+6V_{n+2}^{(s)}+4V_{n+1}^{(s)}+V_n^{(s)}=0\quad(n\in\mathbb{Z}).$$

Clearly we also have

$$v_{n+4}^{(s)}-v_{n+3}^{(s)}+6v_{n+2}^{(s)}+4v_{n+1}^{(s)}+v_n^{(s)}=0\quad(n\in\mathbb{Z}).$$

Note that

$$\frac{1}{5}\sum_{\zeta^5=1}\zeta^k=[5\mid k]\quad\text{for any } k\in\mathbb{Z};$$

in particular

$$\frac{1}{5}\sum_{\zeta^5=1}\zeta^{1-2s}=0=\frac{1}{5}\sum_{\zeta^5=1}\zeta^{-2s}.$$

Thus

$$V_0^{(s)}=\frac{1}{5}\left(\sum_{\zeta^5=1}\zeta^{1-2s}-\sum_{\zeta^5=1}\zeta^{-2s}\right)=0=v_0^{(s)}$$

and

$$\begin{aligned}V_1^{(s)}=&\frac{1}{5}\sum_{\zeta^5=1}(\zeta^{1-2s}-\zeta^{-2s})(1+2\zeta+\zeta^2)\\=&\frac{1}{5}\sum_{\zeta^5=1}(\zeta^{3-2s}+\zeta^{2-2s})=[s=1]=v_1^{(s)}.\end{aligned}$$

Also,

$$\begin{aligned}V_2^{(s)}=&\frac{1}{5}\sum_{\zeta^5=1}(\zeta^{1-2s}-\zeta^{-2s})(1+4\zeta+6\zeta^2+4\zeta^3+\zeta^4)\\=&\frac{1}{5}\sum_{\zeta^5=1}(3\zeta^{4-2s}+2\zeta^{3-2s}-2\zeta^{2-2s})=-2[s=1]+3[s=2]=v_2^{(s)}\end{aligned}$$

and

$$\begin{aligned}V_3^{(s)} =&\frac{1}{5}\sum_{\zeta^5=1}(\zeta^{1-2s}-\zeta^{-2s})(1+6\zeta+15\zeta^2+20\zeta^3+15\zeta^4+6\zeta^5+\zeta^6)\\ =&\frac{1}{5}\sum_{\zeta^5=1}(\zeta^{1-2s}-\zeta^{-2s})(7\zeta+15\zeta^2+20\zeta^3+15\zeta^4)\\ =&[s=1](7-15)+[s=2](20-15)=v_3^{(s)}.\end{aligned}$$

By the above, $V_n^{(s)}=v_n^{(s)}$ for all $n\in\mathbb{N}$.

Now fix $d\in\mathbb{N}$. For any algebraic integer ζ, we have $(1+\zeta)^{p^a}\equiv 1+\zeta^{p^a} \pmod p$ and hence

$$\begin{aligned}&(1+\zeta)^{2(p^a+d)}-(1+\zeta)^{2d}\\ \equiv&(1+\zeta)^{2d}((1+\zeta^{p^a})^2-1)\\ \equiv&\sum_{k=0}^{2d}\binom{2d}{k}(\zeta^{k+2p^a}+2\zeta^{k+p^a}) \pmod p.\end{aligned}$$

Thus

$$\begin{aligned}&5(V_{p^a+d}^{(s)}-V_d^{(s)})\\ =&\sum_{\zeta^5=1}(\zeta^{1-2s}-\zeta^{-2s})((1+\zeta)^{2p^a+2d}-(1+\zeta)^{2d})\\ \equiv&\sum_{\zeta^5=1}(\zeta^{1-2s}-\zeta^{-2s})\sum_{k=0}^{2d}\binom{2d}{k}(\zeta^{k+2p^a}+2\zeta^{k+p^a})\\ \equiv&5\sum_{k+2p^a\equiv 2s-1 \ (\mathrm{mod}\ 5)}\binom{2d}{k}-5\sum_{k+2p^a\equiv 2s \ (\mathrm{mod}\ 5)}\binom{2d}{k}\\ &+10\sum_{k+p^a\equiv 2s-1 \ (\mathrm{mod}\ 5)}\binom{2d}{k}-10\sum_{k+p^a\equiv 2s \ (\mathrm{mod}\ 5)}\binom{2d}{k} \pmod p.\end{aligned}$$

It is known that

$$5\sum_{k\equiv r \ (\mathrm{mod}\ 5)}\binom{2d}{k}-2^{2d}=[5\mid d-r]2L_{2d}+\left(\frac{d-r}{5}\right)L_{2d-(\frac{d-r}{5})}$$

for all $r\in\mathbb{Z}$. (Cf. [S92], [SS], [Su02] and [Su08].) Therefore $5(V_{p^a+d}^{(s)}-V_d^{(s)})$ is congruent to the right-hand side of the congruence in Lemma 5.1(ii) modulo p. So the desired congruence follows.

The proof of Lemma 5.1 is now complete. □

Remark 5.1. On April 27, 2009, the author sent a message [Su09] to Number Theory List in which he raised the following conjecture: Let p be a prime and N_p denote the number of solutions of the the congruence $x^4 - x^3 + 6x^2 + 4x + 1 \equiv 0 \pmod{p}$. If $p \equiv 1 \pmod{10}$ and $p \neq 11$, then $N_p = 4$; if $p \equiv 3, 7, 9 \pmod{10}$ then $N_p = 0$. Also,

$$v_p^{(1)} = u_{p+2} - 3u_{p+1} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv 1, 3 \pmod{10}, \\ -2 \pmod{p} & \text{if } p \equiv 7 \pmod{10}, \\ 0 \pmod{p} & \text{if } p \equiv 9 \pmod{10}. \end{cases}$$

In May 2009, the conjecture was confirmed by K. Buzzard [B], R. Chapman [Ch], E.H. Goins [G] and also D. Brink, K. S. Chua, K. Foster and F. Lemmermeyer (personal communications); all of them realized Lemma 5.1(i). The author would like to thank these cleaver mathematicians for their solutions to the problem.

Lemma 5.2. *Let $p \neq 5$ be a prime and let $a \in \mathbb{Z}^+$. For $s = 1, 2$ we have*

$$v_{p^a}^{(s)} \equiv [5 \mid p^a - s - 2] - [5 \mid p^a - s] + 2[5 \mid p^a - 2s + 1] - 2[5 \mid p^a - 2s] \pmod{p}.$$

Also,

$$v_{p^a+1}^{(1)} - 1 \equiv \begin{cases} -3 \pmod{p} & \textit{if } p^a \equiv 1 \pmod{5}, \\ 2 \pmod{p} & \textit{if } p^a \equiv -1 \pmod{5}, \\ -1 \pmod{p} & \textit{if } p^a \equiv \pm 2 \pmod{5}; \end{cases}$$

$$v_{p^a+1}^{(2)} \equiv \begin{cases} \pm 3 \pmod{p} & \textit{if } p^a \equiv \pm 1 \pmod{5}, \\ \pm 1 \pmod{p} & \textit{if } p^a \equiv \pm 2 \pmod{5}; \end{cases}$$

$$v_{p^a+2}^{(1)} - v_2^{(1)} \equiv \begin{cases} -6 \pmod{p} & \textit{if } p^a \equiv 1 \pmod{5}, \\ 7 \pmod{p} & \textit{if } p^a \equiv -1 \pmod{5}, \\ 2 \pmod{p} & \textit{if } p^a \equiv 2 \pmod{5}, \\ 3 \pmod{p} & \textit{if } p^a \equiv -2 \pmod{5}; \end{cases}$$

$$v_{p^a+2}^{(2)} - v_2^{(2)} \equiv \begin{cases} 2 \pmod{p} & \textit{if } p^a \equiv 1 \pmod{5}, \\ -3 \pmod{p} & \textit{if } p^a \equiv -1 \pmod{5}, \\ -4 \pmod{p} & \textit{if } p^a \equiv \pm 2 \pmod{5}; \end{cases}$$

$$v_{p^a+3}^{(2)} - v_3^{(2)} \equiv \begin{cases} -18 \pmod{p} & \textit{if } p^a \equiv 1 \pmod{5}, \\ 16 \pmod{p} & \textit{if } p^a \equiv -1 \pmod{5}, \\ -8 \pmod{p} & \textit{if } p^a \equiv 2 \pmod{5}, \\ -5 \pmod{p} & \textit{if } p^a \equiv -2 \pmod{5}; \end{cases}$$

and

$$v_{p^a-1}^{(1)} \equiv \begin{cases} 0 \pmod{p} & \textit{if } p^a \equiv \pm 1 \pmod{5}, \\ \pm 5 \pmod{p} & \textit{if } p^a \equiv \pm 2 \pmod{5}. \end{cases}$$

Proof. Note that for $a\in\mathbb{Z}$ we have

$$\left(\frac{a}{5}\right)L_{-(\frac{a}{5})}=-\left(\frac{a}{5}\right)^2=-[5\nmid a]=[5\mid a]-1.$$

Thus Lemma 5.1 in the case $d=0$ yields the first congruence in Lemma 5.2. We can also apply Lemma with $d=1,2,3$ to get the five congruences in Lemma 5.2 following the first one.

Now we deduce the last congruence in Lemma 5.2. By the proof of Lemma 5.1,

$$5v_{p^a-1}^{(1)}=5V_{p^a-1}^{(1)}=\sum_{\zeta^5=1}(\zeta^{-1}-\zeta^{-2})((1+\zeta)^{2(p^a-1)}\pmod p).$$

For any primitive 5th root ζ of unity, clearly

$$(1+\zeta)(\zeta+\zeta^3)=\zeta+\zeta^3+\zeta^2+\zeta^4=-1$$

and hence

$$(1+\zeta)^{-2}=(-\zeta-\zeta^3)^2=2\zeta^4+\zeta^2+\zeta=\zeta^4-\zeta^3-1;$$

also

$$(\zeta^{-1}-\zeta^{-2})(\zeta^4-\zeta^3-1)=\zeta-\zeta^{-1}-2\zeta^2+2\zeta^{-2}$$

and

$$(1+\zeta)^{2p^a}\equiv(1+\zeta^{p^a})^2\equiv1+2\zeta^{p^a}+\zeta^{2p^a}\pmod p.$$

Therefore

$$\begin{aligned}5v_{p^a-1}^{(1)}&\equiv\sum_{\zeta^5=1}(\zeta-\zeta^{-1}-2\zeta^2+2\zeta^{-2})(1+2\zeta^{p^a}+\zeta^{2p^a})\\&\equiv\sum_{\zeta^5=1}(\zeta-\zeta^{-1}-2\zeta^2+2\zeta^{-2})(2\zeta^{p^a}+\zeta^{2p^a})\\&\equiv\begin{cases}5((-1)\times2+2\times1)\pmod p&\text{if } p^a\equiv1\pmod 5,\\5(1\times2+(-2)\times1)\pmod p&\text{if } p^a\equiv-1\pmod 5,\\5(2\times2+1\times1)\pmod p&\text{if } p^a\equiv2\pmod 5,\\5(-2\times2+(-1)\times1)\pmod p&\text{if } p^a\equiv-2\pmod 5.\end{cases}\end{aligned}$$

This yields the last congruence in Lemma 5.2. We are done. □

Proof of Theorem 1.8. For the polynomial

$$x^4-x^3+6x^2+4x+1=(x+1)^4-5x^3,$$

its discriminant is $5^3\times11^2$.

(i) Suppose that $p \neq 11$. Then p does not divide $D((x+1)^4 - 5x^3)$. For any $n \in \mathbb{Z}$ we have

$$11u_n = (3u_{n+1} + 2u_n) - 3(u_{n+1} - 3u_n) = v_n^{(2)} - 3v_{n-1}^{(1)}.$$

Let $d \in \{-2, \ldots, p^a\}$. Applying Theorem 2.1(ii) with $h = 4$ and $m = 5$, we get

$$S_d \equiv u_{p^a+d+2} - u_{d+2} \pmod{p}$$

and thus

$$11S_d \equiv (v_{p^a+d+2}^{(2)} - v_{d+2}^{(2)}) - 3(v_{p^a+d+1}^{(1)} - v_{d+1}^{(1)}) \pmod{p}.$$

Therefore, with the help of Lemma 5.2, we have

$$\begin{aligned} 11S_0 \equiv&(v_{p^a+2}^{(2)} - v_2^{(2)}) - 3(v_{p^a+1}^{(1)} - v_1^{(1)}) \\ \equiv&\begin{cases} 2 - 3(-3) \pmod{p} & \text{if } p^a \equiv 1 \pmod{5}, \\ -3 - 3 \times 2 \pmod{p} & \text{if } p^a \equiv -1 \pmod{5}, \\ -4 - 3(-1) \pmod{p} & \text{if } p^a \equiv \pm 2 \pmod{5}; \end{cases} \end{aligned}$$

and

$$\begin{aligned} 11S_1 \equiv&(v_{p^a+3}^{(2)} - v_3^{(2)}) - 3(v_{p^a+2}^{(1)} - v_2^{(1)}) \\ \equiv&\begin{cases} -18 - 3(-6) \pmod{p} & \text{if } p^a \equiv 1 \pmod{5}, \\ 16 - 3 \times 7 \pmod{p} & \text{if } p^a \equiv -1 \pmod{5}, \\ -8 - 3 \times 2 \pmod{p} & \text{if } p^a \equiv 2 \pmod{5}, \\ -5 - 3 \times 3 \pmod{p} & \text{if } p^a \equiv -2 \pmod{5}. \end{cases} \end{aligned}$$

Also,

$$\begin{aligned} 11S_{-1} \equiv&(v_{p^a+1}^{(2)} - v_1^{(2)}) - 3(v_{p^a}^{(1)} - v_0^{(1)}) = v_{p^a+1}^{(2)} - 3v_{p^a}^{(1)} \\ \equiv&\begin{cases} 3 - 3 \times 1 \pmod{p} & \text{if } p^a \equiv 1 \pmod{5}, \\ -3 - 3 \times 0 \pmod{p} & \text{if } p^a \equiv -1 \pmod{5}, \\ 1 - 3(-2) \pmod{p} & \text{if } p^a \equiv 2 \pmod{5}, \\ -1 - 3 \times 1 \pmod{p} & \text{if } p^a \equiv -2 \pmod{p}. \end{cases} \end{aligned}$$

and

$$\begin{aligned} 11S_{-2} \equiv&(v_{p^a}^{(2)} - v_0^{(2)}) - 3(v_{p^a-1}^{(1)} - v_{-1}^{(1)}) = v_{p^a}^{(2)} - 3v_{p^a-1}^{(1)} \\ \equiv&\begin{cases} 0 - 3 \times 0 \pmod{p} & \text{if } p^a \equiv 1 \pmod{5}, \\ -1 - 3 \times 0 \pmod{p} & \text{if } p^a \equiv -1 \pmod{5}, \\ -1 - 3 \times 5 \pmod{p} & \text{if } p^a \equiv 2 \pmod{5}, \\ 2 - 3(-5) \pmod{p} & \text{if } p^a \equiv -2 \pmod{p}. \end{cases} \end{aligned}$$

This proves part (i).

(ii) Part (ii) follows from the first congruence in Theorem 2.1(i) with $h=3$ and $m=5$.

(iii) As $C_k^{(3)}=\binom{4k}{k}-3\binom{4k}{k-1}$ and $\bar{C}_k^{(3)}=3\binom{4k}{k}-3\binom{4k}{k+1}$ for any $k\in\mathbb{N}$, if $p\neq 11$ then we can obtain the last two congruences in Theorem 1.8 by using the congruences on $S_0,S_{\pm1}$ mod p in part (i).

Below we handle the case $p=11$. This time we turn our resort to Theorem 2.1(i). By (2.4) in the case $h=3$ and $m=5$,

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\frac{C_k^{(3)}}{5^k}=\sum_{k=0}^{p^a-1}\frac{\binom{4k}{k}}{5^k}-3\sum_{k=0}^{p^a-1}\frac{\binom{4k}{k-1}}{5^k}\\ \equiv&-\sum_{r+1}^{4}\binom{4}{r+1}(u_{2-rp^a}-3u_{2-1-rp^a})=-\sum_{r=1}^{3}\binom{4}{r+1}v_{-rp^a}^{(1)}\pmod p.\end{aligned}$$

and

$$\begin{aligned}&\sum_{k=0}^{p^a-1}\frac{\bar{C}_k^{(3)}}{5^k}=3\sum_{k=0}^{p^a-1}\frac{\binom{4k}{k}}{5^k}-\sum_{k=0}^{p^a-1}\frac{\binom{4k}{k+1}}{5^k}\\ \equiv&-\sum_{r+1}^{4}\binom{4}{r+1}(3u_{2-rp^a}-u_{2+1-rp^a})=\sum_{r=1}^{3}\binom{4}{r+1}v_{1-rp^a}^{(1)}\pmod p.\end{aligned}$$

By the proof of Lemma 5.1, $v_n^{(1)}=V_n^{(1)}$ for all $n\in\mathbb{Z}$. Since $p^a=11^a\equiv 1\pmod 5$, if ζ is a 5th root of unity then

$$(1+\zeta)^{-2rp^a}\equiv(1+\zeta^{p^a})^{-2r}=(1+\zeta)^{-2r}\pmod p.$$

Thus

$$v_{-rp^a}^{(1)}=V_{-rp^a}^{(1)}\equiv V_{-r}^{(1)}=v_{-rp^a}^{(1)}\pmod p$$

and

$$v_{1-rp^a}^{(1)}=V_{1-rp^a}^{(1)}\equiv V_{1-r}^{(1)}=v_{1-rp^a}^{(1)}\pmod p.$$

Therefore

$$\begin{aligned}\sum_{k=0}^{p^a-1}\frac{C_k^{(3)}}{5^k}\equiv&-\sum_{r=1}^{3}\binom{4}{r+1}v_{-r}^{(1)}=-(6v_{-1}^{(1)}+4v_{-2}^{(1)}+v_{-3}^{(1)})\\ \equiv&v_1^{(1)}-v_0^{(1)}=u_3-3u_2-(u_2-3u_1)=1\pmod p.\end{aligned}$$

and

$$\begin{aligned}\sum_{k=0}^{p^a-1}\frac{\bar{C}_k^{(3)}}{5^k}\equiv&\sum_{r=1}^{3}\binom{4}{r+1}v_{1-r}^{(1)}=6v_0^{(1)}+4v_{-1}^{(1)}+v_{-2}^{(1)}\\ \equiv&v_1^{(1)}-v_2^{(1)}=u_3-3u_2-(u_4-3u_3)=3\pmod p.\end{aligned}$$

In view of the above, we have completed the proof of Theorem 1.8. □

6. Proof of Theorem 1.9

Proof of Theorem 1.9. Let $U_0 = U_1 = U_2 = 0$, $U_3 = 1$ and

$$U_{n+4} + \left(4 - \frac{4^4}{3^3}\right) U_{n+3} + 6U_{n+2} + 4U_{n+1} + U_n = 0 \quad \text{for } n \in \mathbb{Z}.$$

Observe that

$$(1+x)^4 - \frac{4^4}{3^3}x^3 = (x-3)^2 \left(x - \frac{\alpha}{27}\right)\left(x - \frac{\beta}{27}\right),$$

where $\alpha + \beta = -14$ and $\alpha\beta = 81$. Let $u_n = u_n(-14, 81)$ and $v_n = v_n(-14, 81)$ for $n \in \mathbb{Z}$. By induction,

$$2^5 U_n = (6n-11)3^{n-1} + 3^{-3(n-1)}(5u_n - 11u_{n-1}) \quad \text{for } n \in \mathbb{Z}.$$

This, together with Fermat's little theorem and Theorem 2.1(i) with $h = 3$ and $m = 4^4/3^3$, yields that if $d \in \{-2, \dots, p^a\}$ then

$$\begin{aligned}
&-\sum_{k=0}^{p^a-1} \frac{3^{3k}}{4^{4k}} \binom{4k}{k+d} \\
\equiv& 6U_{2+d-p^a} + 4U_{2+d-2p^a} + U_{2+d-3p^a} \\
\equiv& \frac{67}{64}(6d+1)3^{d-2} + \frac{5(2u_{d+2-p^a} + 36u_{d+2-2p^a} + 3^5 u_{d+2-3p^a})}{64 \times 3^{2d-1}} \\
&- \frac{11(2u_{d+1-p^a} + 36u_{d+1-2p^a} + 3^5 u_{d+1-3p^a})}{64 \times 3^{2d-1}} \pmod p.
\end{aligned}$$

Let n be any integer. Note that $v_n = 2u_{n+1} + 14u_n$ and $\Delta := (-14)^2 - 4 \times 81 = -2^7$. Applying Lemma 3.1 we get

$$u_{n-p^a} \equiv -\frac{7}{81}\left(1 + \left(\frac{-2}{p^a}\right)\right)u_n - \left(\frac{-2}{p^a}\right)\frac{u_{n+1}}{81} \pmod p.$$

It follows that

$$u_{n-2p^a} = u_{(n-p^a)-p^a} \equiv \frac{17 + 98(\frac{-2}{p^a})}{81^2}u_n + \frac{14}{81^2}\left(\frac{-2}{p^a}\right)u_{n+1} \pmod p$$

and

$$u_{n-3p^a} = u_{(n-p^a)-2p^a} \equiv \frac{(329 - 805(\frac{-2}{p^a}))u_n - 115(\frac{-2}{p^a})u_{n+1}}{81^3} \pmod p.$$

Combining the above, for any $d = -2, \ldots, p^a$ we obtain the congruence

$$\begin{aligned} &64\sum_{k=0}^{p^a-1}\frac{3^{3k}}{4^{4k}}\binom{4k}{k+d} + 67(6d+1)3^{d-2} \\ \equiv &\frac{(1705-482(\frac{-2}{p^a}))u_{d+1} - (775+46(\frac{-2}{p^a}))u_{d+2}}{27^{d+2}} \pmod p. \end{aligned} \tag{6.1}$$

Putting $d = 0, -1$ in (6.1) we get

$$\sum_{k=0}^{p^a-1}\frac{3^{3k}}{4^{4k}}\binom{4k}{k} \equiv \frac{44+(\frac{-2}{p^a})}{288} \pmod p$$

and

$$3\sum_{k=0}^{p^a-1}\frac{3^{3k}}{4^{4k}}\binom{4k}{k-1} \equiv -\frac{220+23(\frac{-2}{p^a})}{288} \pmod p.$$

It follows that

$$\sum_{k=0}^{p^a-1}\frac{3^{3k}}{4^{4k}}C_k^{(3)} = \sum_{k=0}^{p^a-1}\frac{3^{3k}}{4^{4k}}\left(\binom{4k}{k} - 3\binom{4k}{k-1}\right) \equiv \frac{(\frac{-2}{p^a})-1}{12} \pmod p.$$

By Lemma 3.1,

$$2u_{p^a+1} \equiv -14u_1 + \left(\frac{\Delta}{p^a}\right)v_1 = -14 - 14\left(\frac{-2}{p^a}\right) \pmod p$$

and

$$2u_{p^a+2} \equiv -14u_2 + \left(\frac{\Delta}{p^a}\right)v_2 = 196 + 34\left(\frac{-2}{p^a}\right) \pmod p.$$

Thus, by taking $d = p^a$ in (6.1) we obtain the second congruence in Theorem 1.9. We are done. $\square$

References

[B] K. Buzzard, *Re: a conjecture on a 4th recurrence mod p*, A Message to Number Theory List (May, 2009), on-line version is available from the website `listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0905&L=nmbrthry&T=0&P=179`.

[C] L. Carlitz, *A theorem of Stickelberger*, Math. Scand. **1** (1953), 82–84.

[Ch] R. Chapman, *Re: a conjecture on a 4th recurrence mod p*, A Message to Number Theory List (May, 2009), on-line version is available from the website `listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0905&L=nmbrthry&T=0&P=305`.

[G] E. H. Goins, *Re: a conjecture on a 4th recurrence mod p*, A Message to Number Theory List (May, 2009), on-line version is available from the website `listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0905&L=nmbrthry&T=0&P=431`.

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

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in math.; 84), 2nd ed., Springer, New York, 1990.

[HS] H. Hu and Z. W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478.

[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. 2, Cambridge Univ. Press, Cambridge, 1999.

[S92] Z.-H. Sun, *Combinatorial sum* $\sum_{k\equiv r \pmod m}\binom{n}{k}$ *and its applications in number theory* (I), Nanjing Univ. J. Math. Biquarterly **9** (1992), no. 2, 227–240.

[S03] Z. H. Sun, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102** (2003), 41–89.

[S98] Z. H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291–335.

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

[Su02] 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.

[Su08] Z. W. Sun, *On sums of binomial coefficients and their applications*, Discrete Math. **308** (2008), 4231–4245.

[Su09] Z. W. Sun, *A conjecture on a 4th recurrence mod p*, A Message to Number Theory List (April 27, 2009), on-line version is available from the website `listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0904&L=nmbrthry&T=0&P=1549`.

[ST1] Z. W. Sun and R. Tauraso, *On some new congruences for binomial coefficients*, Acta Arith., to appear.

[ST2] Z. W. Sun and R. Tauraso, *New congruences for central binomial coefficients*, Adv. in Math., to appear. `http://arxiv.org/abs/0805.0563`.

[ZPS] L. Zhao, H. Pan and Z. W. Sun, *Some congruences for the second-order Catalan numbers*, Proc. Amer. Math. Soc., in press.