Reprint from

ISSN 2220-5438

Moscow Journal of Combinatorics and Number Theory

URSS

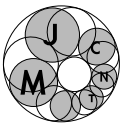
МФТИ

Volume 7 • Issue 4 2017

Moscow Journal of Combinatorics and Number Theory Volume 7 • Issue 4 2017

URSS

Moscow Journal
of Combinatorics
and Number Theory
2017, vol. 7, iss. 4,
pp. 58–87, [pp. 326–355]



Combinatorial Sums $\sum_{k\equiv r \pmod m} \binom{n}{k} a^k$ and Lucas Quotients

Jiangshuai Yang, Yingpu Deng (Beijing):
Received 26.10.16

Abstract: In this paper, we study the combinatorial sum

$$\sum_{k\equiv r (\mathrm{mod}\ m)} \binom{n}{k} a^k.$$

By studying this sum, we obtain new congruences for Lucas quotients of two infinite families of Lucas sequences. Only for three Lucas sequences, there are such known results. Using these general congruences, one can get some new concrete congruences modulo primes, for example,

$$\sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{k} \equiv -\frac{3^p-3}{p} \pmod p,$$

$$\sum_{k=1}^{[\frac{p+1}{3}]} \frac{(-8)^k}{12k-8} + \sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{6k-2} \equiv \left(\frac{-3}{p}\right)\left(\frac{2^p-2}{p} - \frac{3^{p-1}-1}{p}\right) \pmod p,$$

where $p>3$ is a prime.

Keywords: Binomial coefficient, Combinatorial sum, Congruence, Fermat quotient, Lucas quotient

AMS Subject Classification: 11B39, 11B37, 05A10

Received: 26.10.16

1. Introduction

Let $\{F_n\}_{n\geq 0}$ be the Fibonacci sequence, i.e.,

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+1} = F_n + F_{n-1} \text{ for } n \geq 1.$$

For example, $F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5$, etc. It is well-known that

$$p \mid F_{p-\left(\frac{p}{5}\right)},$$

where p is an arbitrary prime, and $\left(\frac{p}{5}\right)$ is the Legendre symbol. We know that

$$\left(\frac{p}{5}\right) = \begin{cases} 0, & \text{if } p = 5, \\ 1, & \text{if } p \equiv \pm 1 \pmod 5, \\ -1, & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

For example, we have that $2 \mid F_3$,$3 \mid F_4$ and $5 \mid F_5$. In 1960 Wall [10] posed the problem of whether there exists a prime p such that

$$p^2 \mid F_{p-\left(\frac{p}{5}\right)}.$$

Up to now this is still open.

An idea related to Wall's problem is to consider the Fibonacci quotient

$$\frac{F_{p-\left(\frac{p}{5}\right)}}{p}.$$

In 1982 Williams [11] obtained this quotient as

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

where $p \neq 5$ is an odd prime, and $\left[\frac{p}{5}\right]$ is the integral part of $\frac{p}{5}$, i.e., the largest integer $\leq \frac{p}{5}$.

We know that the Fibonacci sequence is a special Lucas sequence. In general, let $A, B \in \mathbb{Z}$, the Lucas sequence $\{u_n\}_{n\geq 0}$ is defined as

$$u_0 = 0, u_1 = 1, u_{n+1} = Bu_n - Au_{n-1} \text{ for } n \geq 1.$$

Thus, when $A = -1$ and $B = 1$, we get the Fibonacci sequence. Let $D = B^2 - 4A$ and let $p \nmid A$ be an odd prime. It is well-known that

$$p \mid u_{p-\left(\frac{D}{p}\right)}.$$

So, similarly, we can consider the Lucas quotient

$$\frac{u_{p-\left(\frac{D}{p}\right)}}{p} \pmod p,$$

and we hope that we can obtain some expression as Williams' for Fibonacci quotient.

Williams' method is to consider the sum

$$\sum_{k\equiv r (\mathrm{mod}\ 5)} \binom{p}{k},$$

where r is an integer and $\binom{p}{k}$ is the binomial coefficient with the convention $\binom{p}{k} = 0$ for $k < 0$ or $k > p$. Williams did not give any explicit formula for this sum, but he used the properties of the sum to deduce his congruence. Along this line, Z.-H Sun [4–6], Z.-W Sun [8, 9] and Z.-H Sun and Z.-W Sun [7] studied the sum

$$\sum_{k\equiv r (\mathrm{mod}\ m)} \binom{n}{k},$$

where n, m and r are integers with $n > 0$ and $m > 0$. They gave the formulae of the value of the sum for small m and obtained congruences for two new Lucas sequences. One is the Pell sequence $\{P_n\}_{n\geq 0}$ which is defined as

$$P_0 = 0, P_1 = 1, P_{n+1} = 2P_n + P_{n-1} \text{ for } n \geq 1.$$

Pell sequence is the Lucas sequence with $A = -1$ and $B = 2$. Z.-H Sun's congruence is

$$\frac{P_{p-\left(\frac{2}{p}\right)}}{p} \equiv (-1)^{\frac{p-1}{2}} \sum_{k=1}^{\left[\frac{p+1}{4}\right]} \frac{(-1)^k}{2k-1} \pmod p,$$

where p is an odd prime, see ([5] Theorem 2.5). Z.-H Sun obtained this congruence by studying the above sum with $m = 8$. Z.-W Sun [8] also studied the above sum with $m = 8$ to deduce a congruence for primes. Z.-H Sun and Z.-W Sun [7] obtained a new congruence for the Fibonacci quotient by studying the above sum with $m = 10$.

The second new Lucas sequence is the sequence $\{S_n\}_{n\geq 0}$ which is defined as

$$S_0 = 0, S_1 = 1, S_{n+1} = 4S_n - S_{n-1} \text{ for } n \geq 1.$$

This sequence is the Lucas sequence with $A = 1$ and $B = 4$. Z.-W Sun [9] obtained

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{3^k}{k} \equiv \sum_{k=1}^{\left[\frac{p}{6}\right]} \frac{(-1)^k}{k} \equiv -6\left(\frac{2}{p}\right)\frac{S_{\overline{p}}}{p} - q_p(2) \pmod p,$$

where $p > 3$ is a prime, $\overline{p} = \frac{p-\left(\frac{3}{p}\right)}{2}$ and $q_p(2) = \frac{2^{p-1}-1}{p}$ is the Fermat quotient of 2 with respect to p. See ([9] Theorem 3). Z.-W Sun obtained this congruence by studying the above sum with $m = 12$.

So far, except the above mentioned three Lucas sequences, there is no any known congruence for new Lucas quotients. Noticed that, we do not consider the case where $D = B^2 - 4A$ is a perfect square. If $D = B^2 - 4A$ is a perfect square, then Lucas quotients degenerate to Fermat quotients. In this paper, we study the more general sum

$$\sum_{k\equiv r(\text{mod } m)} \binom{n}{k} a^k. \tag{1}$$

When $a = 1$, this sum is that considered by Williams, Z.-H Sun and Z.-W Sun. By studying this sum, we obtain new congruences for Lucas quotients of two infinite families of Lucas sequences, see Theorems 4.2 and 5.2. Using these general

congruences, one can get some new concrete congruences modulo primes, for example,

$$\sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{k} \equiv -\frac{3^p-3}{p} \pmod{p},$$

$$\sum_{k=1}^{[\frac{p+1}{3}]} \frac{(-8)^k}{12k-8} + \sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{6k-2} \equiv \left(\frac{-3}{p}\right)\left(\frac{2^p-2}{p} - \frac{3^{p-1}-1}{p}\right) \pmod{p},$$

where $p > 3$ is a prime. See Corollaries 4.2 and 4.3.

Another motivation of this paper is the result in [2]. Deng and Pan [2] connected this combinatorial sum with integer factorization for the first time and they proved that, when n is a composite number, for every integer a with $\gcd(n, a) = 1$, there exists a pair (m, r) of integers such that the sum (1) has a nontrivial greatest common divisor with n.

Integer factorization is a famous and very important computational problem, and it is the security foundation of the famous public-key cryptosystem RSA [3]. So it is worthwhile to make a systematic research of the combinatorial sum for a general a.

Below, we briefly describe the achievements of the present paper. Because they are quite large in number and technical in their hypotheses, we cannot mention all of them. First, we obtain explicit recurrent relations for the sum (1), which have order $m-1$ for odd m and order $m-2$ for even m. However, for $m = 6$, the characteristic polynomial of the recurrent relation is a product of two polynomials of degree two. Hence, for $m = 3,4$ and 6, we can obtain the recurrent relations of order two for the sum (1). In these cases, we can give the formulae of the sum (1) via relevant Lucas sequences. Second, using these formulae, we obtain new congruences for Lucas quotients of two infinite families of Lucas sequences, i.e., $A = a^2 - a + 1, B = 2 - a$ or $A = a^2 + 1, B = 2$, where a is an arbitrary integer. By specifying the value of a, we can obtain numerous congruences for new concrete Lucas quotients.

The paper is organized as follows. We give some necessary preliminaries in Section 2. We deduce the recurrent relation for the combinatorial sum in Section 3. We consider the calculation of the combinatorial sum and give some applications when $m = 3,4,6$ in Sections 4,5,6, respectively.

2. Preliminaries

Notational conventions: We denote by $\mathbb{C}, \mathbb{R}, \mathbb{Z}$ respectively the complex numbers, the reals and the integers. For $x \in \mathbb{R}$, we denote by $[x]$ the integral part of x, i.e., the largest integer $\leq x$.

First we recall some well-known facts about Lucas sequences. Let $A, B \in \mathbb{Z}$. We define Lucas sequences $\{u_n\}_{n\geq 0}$ and $\{v_n\}_{n\geq 0}$ as

$$u_0 = 0, u_1 = 1, u_{n+1} = Bu_n - Au_{n-1} \text{ for } n \geq 1;$$
$$v_0 = 2, v_1 = B, v_{n+1} = Bv_n - Av_{n-1} \text{ for } n \geq 1.$$

The proof of the following two lemmas can be found in [1].

LEMMA 2.1. *Let $D = B^2 - 4A$ and α, β be the two complex roots of $x^2 - Bx + A = 0$. Then we have*

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad v_n = \alpha^n + \beta^n;$$
$$v_n = u_{n+1} - Au_{n-1} = Bu_n - 2Au_{n-1} = 2u_{n+1} - Bu_n;$$
$$Du_n = v_{n+1} - Av_{n-1} = Bv_n - 2Av_{n-1} = 2v_{n+1} - Bv_n;$$
$$u_{2n} = u_n v_n, \quad u_{2n+1} = u_{n+1}^2 - Au_n^2;$$
$$v_{2n} = v_n^2 - 2A^n, \quad v_n^2 - Du_n^2 = 4A^n.$$

LEMMA 2.2. *Let $\varepsilon = \left(\frac{D}{p}\right)$ and $p \nmid A$ be an odd prime. Then we have*

$$u_{p-\varepsilon} \equiv 0 \pmod p, \quad u_p \equiv \varepsilon \pmod p.$$

DEFINITION 2.1. Let n, m, r and a be integers with $n > 0$ and $m > 0$. We define

$$\left[\begin{matrix} n \\ r \end{matrix}\right]_m (a) := \sum_{\substack{k=0 \\ k\equiv r (\mathrm{mod} m)}}^{n} \binom{n}{k} a^k,$$

where $\binom{n}{k}$ is the binomial coefficient with the convention $\binom{n}{k} = 0$ for $k < 0$ or $k > n$. Let p be an odd prime and m, r and a be integers with $m > 0$. We define

$$K_{p,m,r}(a) := \sum_{\substack{k=1 \\ k\equiv r (\mathrm{mod} m)}}^{p-1} \frac{(-a)^k}{k}.$$

LEMMA 2.3. *With notation as above, we have*:

(1) $\sum_{r=0}^{m-1} \begin{bmatrix} n \\ r \end{bmatrix}_m (a) = (1+a)^n$;

(2) $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ *for* $0 \le k \le p-1$;

(3) $\begin{bmatrix} p \\ r \end{bmatrix}_m (a) \equiv \delta_{0\equiv r(m)} + \delta_{p\equiv r(m)} a^p - pK_{p,m,r}(a) \pmod{p^2}$,

where

$$\delta_{0\equiv r(m)} = \begin{cases} 1, & \text{if } 0 \equiv r \pmod{m} \text{ holds}, \\ 0, & \text{otherwise}, \end{cases}$$

and $\delta_{p\equiv r(m)}$ *has the similar meaning.*

PROOF. (1) is obvious.

(2) If $k = 0$, $\binom{p-1}{0} \equiv (-1)^0 \pmod{p}$.

If $1 \le k \le p-1$, $\binom{p-1}{k} = \frac{(p-1)(p-2)\cdots(p-k)}{k!} \equiv (-1)^k \pmod{p}$.

(3) By (2), we have

$$\begin{aligned} \begin{bmatrix} p \\ r \end{bmatrix}_m (a) &= \delta_{0\equiv r(m)} + \delta_{p\equiv r(m)} a^p + \sum_{\substack{k=1 \\ k\equiv r \pmod m}}^{p-1} \binom{p}{k} a^k \\ &= \delta_{0\equiv r(m)} + \delta_{p\equiv r(m)} a^p + \sum_{\substack{k=1 \\ k\equiv r \pmod m}}^{p-1} \frac{p}{k} \binom{p-1}{k-1} a^k \\ &\equiv \delta_{0\equiv r(m)} + \delta_{p\equiv r(m)} a^p - p \sum_{\substack{k=1 \\ k\equiv r \pmod m}}^{p-1} \frac{(-a)^k}{k} \pmod{p^2} \\ &= \delta_{0\equiv r(m)} + \delta_{p\equiv r(m)} a^p - pK_{p,m,r}(a) \pmod{p^2}. \end{aligned}$$

□

Note that, in the above lemma, (2) is well-known and (3) is a generalization of Lemma 1.1 in [4].

DEFINITION 2.2. Let p be an odd prime and x an integer with $p \nmid x$. Fermat quotient is defined as $q_p(x) := \frac{x^{p-1}-1}{p}$. In the sequent, when we meet $q_p(x)$, we always suppose that p is an odd prime and $p \nmid x$.

LEMMA 2.4. *We have*:

(1) $q_p(x) \equiv 2\left(\frac{x}{p}\right) \frac{x^{\frac{p-1}{2}} - \left(\frac{x}{p}\right)}{p} \pmod p$;

(2) $q_p(xy) \equiv q_p(x) + q_p(y) \pmod p$;

(3) $\sum_{r=0}^{m-1} K_{p,m,r}(a) \equiv aq_p(a) - (a+1)q_p(a+1) \pmod p$.

PROOF. (1) From

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

we have

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

(2) From

$$(xy)^{p-1} - 1 = x^{p-1}(y^{p-1} - 1) + (x^{p-1} - 1),$$

we have

$$q_p(xy) \equiv q_p(x) + q_p(y) \pmod p.$$

(3) From Lemma 2.3, we have

$$\begin{aligned} (1+a)^p &= \sum_{r=0}^{m-1} \begin{bmatrix} p \\ r \end{bmatrix}_m (a) \\ &\equiv \sum_{r=0}^{m-1} \left[\delta_{0\equiv r(m)} + \delta_{p\equiv r(m)} a^p - pK_{p,m,r}(a)\right] \pmod{p^2} \\ &\equiv 1 + a^p - p\sum_{r=0}^{m-1} K_{p,m,r}(a) \pmod{p^2}. \end{aligned}$$

Thus we obtain

$$\sum_{r=0}^{m-1} K_{p,m,r}(a) \equiv \frac{1+a^p-(a+1)^p}{p} = aq_p(a)-(a+1)q_p(a+1) \pmod p. \quad \square$$

Note that, in the above lemma, (1) is the Lemma 1.2 in [4].

LEMMA 2.5. *With notation as in Lemmas* 2.1 *and* 2.2. *Let* p *be an odd prime with* $p \nmid DA$. *We have*:

(1) *if* $\varepsilon = 1$, *then* $\frac{v_{p-1}-2}{p} \equiv q_p(A) \pmod p$;

(2) *if* $\varepsilon = -1$, *then* $\frac{v_{p+1}-2A}{p} \equiv Aq_p(A) \pmod p$.

PROOF. By Lemma 2.1, we have $v_n^2 - Du_n^2 = 4A^n$ for $n \geq 0$. Combining this with Lemma 2.2, we have $v_{p-\varepsilon}^2 \equiv 4A^{p-\varepsilon} \pmod{p^2}$. Since it is impossible that $p \mid v_{p-\varepsilon} + 2A^{\frac{p-\varepsilon}{2}}$ and $p \mid v_{p-\varepsilon} - 2A^{\frac{p-\varepsilon}{2}}$, we have

$$v_{p-\varepsilon} \equiv \pm 2\left(\frac{A}{p}\right) A^{\frac{p-\varepsilon}{2}} \pmod{p^2}.$$

If $\varepsilon = 1$, by Lemmas 2.1 and 2.2 we have $v_{p-1} = 2u_p - Bu_{p-1} \equiv 2 \pmod p$. Thus, by Lemma 2.4 (1), we have

$$v_{p-1} \equiv 2\left(\frac{A}{p}\right) A^{\frac{p-1}{2}} \equiv 2 + pq_p(A) \pmod{p^2}.$$

Hence

$$\frac{v_{p-1}-2}{p} \equiv q_p(A) \pmod p,$$

we obtain (1).

If $\varepsilon = -1$, by Lemmas 2.1 and 2.2 we have $v_{p+1} = Bu_{p+1} - 2Au_p \equiv 2A \pmod p$. Thus, by Lemma 2.4 (1), we have

$$v_{p+1} \equiv 2\left(\frac{A}{p}\right) A^{\frac{p+1}{2}} \equiv 2A + Apq_p(A) \pmod{p^2}.$$

Hence

$$\frac{v_{p+1}-2A}{p} \equiv Aq_p(A) \pmod p,$$

we obtain (2). $\square$

3. The Recurrent Relation for $\Delta_m(r, n)$

In this section, we consider the calculation of the sum $\begin{bmatrix} n \\ r \end{bmatrix}_m (a)$. It is easy to see that

$$\begin{bmatrix} n \\ 0 \end{bmatrix}_1 (a) = (1+a)^n, \quad \begin{bmatrix} n \\ r \end{bmatrix}_2 (a) = \frac{(1+a)^n + (-1)^r (1-a)^n}{2}.$$

However, for $m \geq 3$, the calculation is much more difficult.

Throughout the rest of this paper, we fix $a \neq 0, \pm 1$. For any positive integer m, let $\zeta_m = e^{2\pi i/m} \in \mathbb{C}$ be the primitive m-th root of unity.

The following lemma is useful to compute $\begin{bmatrix} n \\ r \end{bmatrix}_m (a)$ when m is small.

LEMMA 3.1. *We have*

$$\begin{bmatrix} n \\ r \end{bmatrix}_m (a) = \frac{1}{m} \sum_{l=0}^{m-1} \zeta_m^{-rl} (1 + a\zeta_m^l)^n.$$

PROOF. Since

$$\begin{aligned} \begin{bmatrix} n \\ r \end{bmatrix}_m (a) &= \sum_{k=0}^{n} \binom{n}{k} a^k \cdot \frac{1}{m} \sum_{l=0}^{m-1} \zeta_m^{(k-r)l} \\ &= \frac{1}{m} \sum_{l=0}^{m-1} \zeta_m^{-rl} \sum_{k=0}^{n} \binom{n}{k} (a\zeta_m^l)^k = \frac{1}{m} \sum_{l=0}^{m-1} \zeta_m^{-rl} (1 + a\zeta_m^l)^n, \end{aligned}$$

the lemma follows. □

PROPOSITION 3.1. *Let* $G_n(x) = \prod_{l=1}^{n} (x - 1 - a\zeta_{2n+1}^l)(x - 1 - a\zeta_{2n+1}^{-l}) := \sum_{s=0}^{2n} b_s x^s$ *for* $n \geq 0$. *Then* $G_n(x) \in \mathbb{Z}[x]$ *and we have*:

(1) $b_0 = \frac{a^{2n+1}+1}{a+1}$, $b_{2n} = 1$ *and* $b_{s-1} - (a+1)b_s = \binom{2n+1}{s}(-1)^{s+1}$ *for* $1 \leq s \leq 2n-1$;

(2) $G_0(x) = 1$ *and* $G_{n+1}(x) = (x-1)^2 G_n(x) + a^{2n+1}(x + a - 1)$ *for* $n \geq 0$.

PROOF. Since $(x-1-a)G_n(x) = (x-1)^{2n+1} - a^{2n+1}$, we have

$$\sum_{s=1}^{2n+1} b_{s-1}x^s - \sum_{s=0}^{2n}(1+a)b_s x^s = x^{2n+1} + \sum_{s=1}^{2n}\binom{2n+1}{s}(-1)^{s+1}x^s - 1 - a^{2n+1}.$$

By comparing coefficients of both sides of the above expression, we obtain (1).

Since $(x-1-a)G_n(x) = (x-1)^{2n+1} - a^{2n+1}$, then $(x-1-a)G_{n+1}(x) + a^{2n+3} = (x-1)^{2n+3} = (x-1)^2\left[(x-1-a)G_n(x) + a^{2n+1}\right]$. Hence $G_{n+1}(x) = (x-1)^2 G_n(x) + a^{2n+1}(x+a-1)$, thus we obtain (2). The assertion $G_n(x) \in \mathbb{Z}[x]$ follows from (2). □

The polynomial $G_n(x)$ depends on a and should be denoted as $G_{n,a}(x)$, for the notational simplification, we omit a. The first few values of $G_n(x)$ are: $G_0(x) = 1$, $G_1(x) = x^2 + (a-2)x + a^2 - a + 1$, $G_2(x) = x^4 + (a-4)x^3 + (a^2 - 3a + 6)x^2 + (a^3 - 2a^2 + 3a - 4)x + a^4 - a^3 + a^2 - a + 1$.

PROPOSITION 3.2. *Let* $Q_n(x) = \prod_{l=1}^{n}(x - 1 - a\zeta_{2n+2}^{l})(x - 1 - a\zeta_{2n+2}^{-l}) := \sum_{s=0}^{2n} c_s x^s$ *for* $n \geq 0$. *Then* $Q_n(x) \in \mathbb{Z}[x]$ *and we have*:

(1) $c_0 = \frac{a^{2n+2}-1}{a^2-1}$, $2c_0 + (a^2-1)c_1 = 2n+2$, $c_{2n-1} = -2n$, $c_{2n} = 1$ *and* $c_{s-2} - 2c_{s-1} + (1-a^2)c_s = \binom{2n+2}{s}(-1)^s$ *for* $2 \leq s \leq 2n-2$;

(2) $Q_0(x) = 1$ *and* $Q_{n+1}(x) = (x-1)^2 Q_n(x) + a^{2n+2}$ *for* $n \geq 0$.

PROOF. Since $(x-1-a)(x-1+a)Q_n(x) = (x-1)^{2n+2} - a^{2n+2}$, we have

$$\sum_{s=2}^{2n+2} c_{s-2}x^s - \sum_{s=1}^{2n+1} 2c_{s-1}x^s + \sum_{s=0}^{2n}(1-a^2)c_s x^s = x^{2n+2} + \sum_{s=1}^{2n+1}\binom{2n+2}{s}(-1)^s x^s + 1 - a^{2n+2}.$$

By comparing coefficients of both sides of the above expression, we obtain (1).

Since $(x-1-a)(x-1+a)Q_n(x) = (x-1)^{2n+2} - a^{2n+2}$, then $(x-1-a)(x-1+a) \times Q_{n+1}(x) + a^{2n+4} = (x-1)^{2n+4} = (x-1)^2\left((x-1-a)(x-1+a)Q_n(x) + a^{2n+2}\right)$. Hence $Q_{n+1}(x) = (x-1)^2 Q_n(x) + a^{2n+2}$, thus we obtain (2). The assertion $Q_n(x) \in \mathbb{Z}[x]$ follows from (2). □

The first few values of $Q_n(x)$ are: $Q_0(x) = 1, Q_1(x) = x^2 - 2x + 1 + a^2$, $Q_2(x) = x^4 - 4x^3 + (a^2+6)x^2 - (2a^2+4)x + a^4 + a^2 + 1 = (x^2 + (a-2)x + a^2 - a + 1) \times (x^2 - (a+2)x + a^2 + a + 1)$.

DEFINITION 3.3. We define

$$\Delta_m(r,n) := \begin{cases} m \begin{bmatrix} n \\ r \end{bmatrix}_m (a) - (1+a)^n, & \text{if } m \text{ is odd,} \\ \\ m \begin{bmatrix} n \\ r \end{bmatrix}_m (a) - (1+a)^n - (-1)^r (1-a)^n, & \text{if } m \text{ is even.} \end{cases}$$

Remark 3.1. *It is obvious that*

$$\Delta_1(r,n) = \Delta_2(r,n) = 0.$$

By Lemma 2.3(1), *it is easy to see that*

$$\sum_{r=0}^{m-1} \Delta_m(r,n) = 0.$$

THEOREM 3.1. *Let m be an odd positive integer, and let $G_{\frac{m-1}{2}}(x) = \sum_{s=0}^{m-1} b_s x^s$ be the same as in Proposition* 3.1. *Then we have $\sum_{s=0}^{m-1} b_s \Delta_m(r, n+s) = 0$.*

PROOF. By Lemma 3.1, we have

$$\begin{aligned} \Delta_m(r,n) &= m \begin{bmatrix} n \\ r \end{bmatrix}_m (a) - (1+a)^n \\ &= \sum_{l=1}^{m-1} \zeta_m^{-rl} (1 + a\zeta_m^l)^n = \sum_{l=1}^{\frac{m-1}{2}} \left[\zeta_m^{-rl} (1 + a\zeta_m^l)^n + \zeta_m^{rl} (1 + a\zeta_m^{-l})^n \right]. \end{aligned}$$

Thus

$$\begin{aligned}
&\sum_{s=0}^{m-1} b_s \Delta_m(r,n+s) = \sum_{s=0}^{m-1} b_s \sum_{l=1}^{\frac{m-1}{2}} \left[\zeta_m^{-rl}(1+a\zeta_m^l)^{n+s} + \zeta_m^{rl}(1+a\zeta_m^{-l})^{n+s}\right] \\
&= \sum_{l=1}^{\frac{m-1}{2}} \zeta_m^{-rl}(1+a\zeta_m^l)^n \sum_{s=0}^{m-1} b_s(1+a\zeta_m^l)^s + \sum_{l=1}^{\frac{m-1}{2}} \zeta_m^{rl}(1+a\zeta_m^{-l})^n \sum_{s=0}^{m-1} b_s(1+a\zeta_m^{-l})^s \\
&= \sum_{l=1}^{\frac{m-1}{2}} \zeta_m^{-rl}(1+a\zeta_m^l)^n G_{\frac{m-1}{2}}(1+a\zeta_m^l) + \sum_{l=1}^{\frac{m-1}{2}} \zeta_m^{rl}(1+a\zeta_m^{-l})^n G_{\frac{m-1}{2}}(1+a\zeta_m^{-l}) \\
&= 0+0=0.
\end{aligned}$$

□

THEOREM 3.2. *Let m be an even positive integer, and let $Q_{\frac{m}{2}-1}(x) = \sum_{s=0}^{m-2} c_s x^s$ be the same as in Proposition 3.2. Then we have $\sum_{s=0}^{m-2} c_s \Delta_m(r, n+s) = 0$.*

PROOF. By Lemma 3.1, we have

$$\begin{aligned}
\Delta_m(r,n) &= m \begin{bmatrix} n \\ r \end{bmatrix}_m (a) - (1+a)^n - (-1)^r(1-a)^n \\
&= \sum_{\substack{l=1 \\ l\neq\frac{m}{2}}}^{m-1} \zeta_m^{-rl}(1+a\zeta_m^l)^n = \sum_{l=1}^{\frac{m}{2}-1} \left[\zeta_m^{-rl}(1+a\zeta_m^l)^n + \zeta_m^{rl}(1+a\zeta_m^{-l})^n\right].
\end{aligned}$$

Thus

$$\begin{aligned}
&\sum_{s=0}^{m-2} c_s \Delta_m(r,n+s) = \sum_{s=0}^{m-2} c_s \sum_{l=1}^{\frac{m}{2}-1} \left[\zeta_m^{-rl}(1+a\zeta_m^l)^{n+s} + \zeta_m^{rl}(1+a\zeta_m^{-l})^{n+s}\right] \\
&= \sum_{l=1}^{\frac{m}{2}-1} \zeta_m^{-rl}(1+a\zeta_m^l)^n \sum_{s=0}^{m-2} c_s(1+a\zeta_m^l)^s + \sum_{l=1}^{\frac{m}{2}-1} \zeta_m^{rl}(1+a\zeta_m^{-l})^n \sum_{s=0}^{m-2} c_s(1+a\zeta_m^{-l})^s \\
&= \sum_{l=1}^{\frac{m}{2}-1} \zeta_m^{-rl}(1+a\zeta_m^l)^n Q_{\frac{m}{2}-1}(1+a\zeta_m^l) + \sum_{l=1}^{\frac{m}{2}-1} \zeta_m^{rl}(1+a\zeta_m^{-l})^n Q_{\frac{m}{2}-1}(1+a\zeta_m^{-l}) \\
&= 0+0=0.
\end{aligned}$$

□

4. $\Delta_3(r, n)$ and Related Lucas Quotients

In this section, we consider the calculation of $\Delta_3(r, n)$.

4.1. General Properties

THEOREM 4.1. *Let $\{u_n\}_{n\geq 0}$ be the Lucas sequence defined as*

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = (2-a)u_n - (a^2 - a + 1)u_{n-1} \text{ for } n \geq 1.$$

Then we have, for $n \geq 1$,

$$\begin{aligned}
\Delta_3(0, n) &= (2-a)u_n - 2(a^2 - a + 1)u_{n-1} = 2u_{n+1} - (2-a)u_n,\\
\Delta_3(1, n) &= (2a-1)u_n + (a^2 - a + 1)u_{n-1} = -u_{n+1} + (a+1)u_n,\\
\Delta_3(2, n) &= (-a-1)u_n + (a^2 - a + 1)u_{n-1} = -u_{n+1} - (2a-1)u_n.
\end{aligned}$$

PROOF. By Lemma 2.1, we have, for $n \geq 1$,

$$\begin{aligned}
(2-a)u_n - 2(a^2 - a + 1)u_{n-1} &= 2u_{n+1} - (2-a)u_n,\\
(2a-1)u_n + (a^2 - a + 1)u_{n-1} &= -u_{n+1} + (a+1)u_n,\\
(-a-1)u_n + (a^2 - a + 1)u_{n-1} &= -u_{n+1} - (2a-1)u_n.
\end{aligned}$$

Since $u_2 = 2 - a$, one can verify the following simple facts:

$$\begin{aligned}
\Delta_3(0,1) &= -a + 2 = (2-a)u_1 - 2(a^2 - a + 1)u_0,\\
\Delta_3(0,2) &= -a^2 - 2a + 2 = (2-a)u_2 - 2(a^2 - a + 1)u_1,\\
\Delta_3(1,1) &= 2a - 1 = (2a-1)u_1 + (a^2 - a + 1)u_0,\\
\Delta_3(1,2) &= -a^2 + 4a - 1 = (2a-1)u_2 + (a^2 - a + 1)u_1,\\
\Delta_3(2,1) &= -a - 1 = (-a-1)u_1 + (a^2 - a + 1)u_0,\\
\Delta_3(2,2) &= 2a^2 - 2a - 1 = (-a-1)u_2 + (a^2 - a + 1)u_1.
\end{aligned}$$

By Theorem 3.1, we have

$$\Delta_3(r, n+2) = (2-a)\Delta_3(r, n+1) - (a^2 - a + 1)\Delta_3(r, n) \text{ for } n \geq 1.$$

Then we can prove the theorem by induction on n. □

Remark 4.1. *Let* $\{v_n\}_{n\geq 0}$ *be the Lucas sequence defined as*

$$v_0 = 2,\ v_1 = 2 - a,\ v_{n+1} = (2-a)v_n - (a^2 - a + 1)v_{n-1} \text{ for } n \geq 1.$$

Then, by the above theorem and Lemma 2.1, *we have, for* $n \geq 1$,

$$\begin{aligned}
\Delta_3(0, n) &= v_n,\\
\Delta_3(1, n) &= -\frac{1}{a}v_n + \frac{a^2 - a + 1}{a}v_{n-1},\\
\Delta_3(2, n) &= -\frac{a-1}{a}v_n - \frac{a^2 - a + 1}{a}v_{n-1}.
\end{aligned}$$

THEOREM 4.2. *Let* $p \nmid 3a(a^3 + 1)$ *be an odd prime,* $\{u_n\}_{n\geq 0}$ *as in Theorem* 4.1, *and* $K_{p,3,r}(a)$ *as in Definition* 2.1. *Then we have*:

(1) *for* $p \equiv 1 \pmod 3$,

$$\begin{aligned}
\frac{u_{p-1}}{p} \equiv &\frac{(2a-1)K_{p,3,0}(a) + (a-2)K_{p,3,1}(a)}{a(a^2 - a + 1)}\\
&- \frac{a-2}{a^2 - a + 1}q_p(a) + \frac{a^2 - 1}{a(a^2 - a + 1)}q_p(a+1) \pmod p;
\end{aligned}$$

(2) *for* $p \equiv 2 \pmod 3$,

$$\frac{u_{p+1}}{p} \equiv \frac{(a-2)K_{p,3,1}(a) - (a+1)K_{p,3,0}(a)}{a} - \frac{a+1}{a}q_p(a+1) \pmod p.$$

PROOF. Since $(2-a)^2 - 4(a^2 - a + 1) = -3a^2$, by Lemma 2.2, we have

$$p \mid u_{p-\left(\frac{-3}{p}\right)}.$$

By Theorem 4.1, we have

$$(2a-1)\Delta_3(0, p) + (a-2)\Delta_3(1, p) = -3a(a^2 - a + 1)u_{p-1}, \tag{2}$$

and

$$(a+1)\Delta_3(0, p) - (a-2)\Delta_3(1, p) = 3au_{p+1}. \tag{3}$$

If $p \equiv 1 \pmod 3$, by Lemma 2.3 (3), we have

$$\Delta_3(0,p) \equiv 3 - 3pK_{p,3,0}(a) - (1+a)^p \pmod{p^2},$$
$$\Delta_3(1,p) \equiv 3a^p - 3pK_{p,3,1}(a) - (1+a)^p \pmod{p^2}.$$

Then, by Eq.(2),

$$a(a^2-a+1)u_{p-1} \equiv p\left[(2a-1)K_{p,3,0}(a) + (a-2)K_{p,3,1}(a)\right] - (a^2-2a)(a^{p-1}-1) + (a^2-1)\left[(a+1)^{p-1}-1\right] \pmod{p^2}.$$

Thus

$$\frac{u_{p-1}}{p} \equiv \frac{(2a-1)K_{p,3,0}(a) + (a-2)K_{p,3,1}(a)}{a(a^2-a+1)} - \frac{a-2}{a^2-a+1}q_p(a) + \frac{a^2-1}{a(a^2-a+1)}q_p(a+1) \pmod p.$$

If $p \equiv 2 \pmod 3$, by Lemma 2.3 (3), we have

$$\Delta_3(0,p) \equiv 3 - 3pK_{p,3,0}(a) - (1+a)^p \pmod{p^2},$$
$$\Delta_3(1,p) \equiv -3pK_{p,3,1}(a) - (1+a)^p \pmod{p^2}.$$

Then, by Eq.(3),

$$au_{p+1} \equiv p\left[(a-2)K_{p,3,1}(a) - (a+1)K_{p,3,0}(a)\right] - \left[(a+1)^p - (a+1)\right] \pmod{p^2}.$$

Thus

$$\frac{u_{p+1}}{p} \equiv \frac{1}{a}\left[(a-2)K_{p,3,1}(a) - (a+1)K_{p,3,0}(a)\right] - \frac{a+1}{a}q_p(a+1) \pmod p. \quad \square$$

Given a value of a, by Theorem 4.2, we can obtain a concrete congruence for a specific Lucas quotient. We provide one such example.

COROLLARY 4.1. *Let* $\{u_n\}_{n\geq 0}$ *be the Lucas sequence defined by*

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = 4u_n - 7u_{n-1} \text{ for } n \geq 1,$$

and $p \neq 3,7$ *be an odd prime. Then we have*

$$\frac{u_{p-1}}{p} \equiv \frac{5}{42}\sum_{k=1}^{\frac{p-1}{3}}\frac{8^k}{k} + \frac{1}{14}\sum_{k=1}^{\frac{p-1}{3}}\frac{8^k}{3k-2} + \frac{4}{7}q_p(2) \pmod p,\ \text{if } p \equiv 1 \pmod 3;$$

$$\frac{u_{p+1}}{p} \equiv \frac{1}{2}\sum_{k=1}^{\frac{p+1}{3}}\frac{8^k}{3k-2} - \frac{1}{6}\sum_{k=1}^{\frac{p-2}{3}}\frac{8^k}{k} \pmod p,\ \text{if } p \equiv 2 \pmod 3.$$

PROOF. Set $a = -2$ in Theorem 4.2. □

4.2. The Case a=2

If $a = 2$, by Theorem 3.1, we have $\Delta_3(r, n+2) = -3\Delta_3(r, n)$ for $n \geq 1$. Thus we have a refinement of Theorem 4.1.

THEOREM 4.3. *Set* $a = 2$. *Let* $\Delta_3(r, n) = 3\begin{bmatrix} n \\ r \end{bmatrix}_3(2) - 3^n$ *for* $n \geq 1$. *Then we have*: *if* n *is odd*,

$$\Delta_3(0, n) = 0,\ \Delta_3(1, n) = -(-3)^{\frac{n+1}{2}},\ \Delta_3(2, n) = (-3)^{\frac{n+1}{2}};$$

if n *is even*,

$$\Delta_3(0, n) = 2\cdot(-3)^{\frac{n}{2}},\ \Delta_3(1, n) = \Delta_3(2, n) = -(-3)^{\frac{n}{2}}.$$

PROOF. Since $a = 2$, by Theorem 3.1, we have $\Delta_3(r, n+2) = -3\Delta_3(r, n)$ for $n \geq 1$. One can verify that

$$\Delta_3(0,1) = 0,\ \Delta_3(1,1) = 3,\ \Delta_3(2,1) = -3;$$
$$\Delta_3(0,2) = -6,\ \Delta_3(1,2) = 3,\ \Delta_3(2,2) = 3.$$

Then we can prove the theorem by induction on n. □

Remark 4.2. *Using the above theorem and without the use of the Quadratic Reciprocity Law, for an odd prime $p > 3$, we can get the Legendre symbol*

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, \text{ if } p \equiv 1 \pmod 3, \\ -1, \text{ if } p \equiv 2 \pmod 3. \end{cases}$$

PROOF. If $p \equiv 1 \pmod 3$, by Theorem 4.3, we have $\Delta_3(1,p) = -(-3)^{\frac{p+1}{2}}$. Since

$$\Delta_3(1,p) = 3\begin{bmatrix} p \\ 1 \end{bmatrix}_3 (2) - 3^p = 3 \sum_{\substack{k=0 \\ k\equiv 1 (\mathrm{mod}\ 3)}}^{p} \binom{p}{k} 2^k - 3^p$$
$$\equiv 3\cdot 2^p - 3^p \equiv 3\cdot 2 - 3 = 3 \pmod p,$$

we have $(-3)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Hence $\left(\frac{-3}{p}\right) = 1$.

If $p \equiv 2 \pmod 3$, by Theorem 4.3, we have $\Delta_3(2,p) = (-3)^{\frac{p+1}{2}}$. Similarly, we can obtain $\left(\frac{-3}{p}\right) = -1$. □

COROLLARY 4.2. *Let $p > 3$ be an odd prime. Then we have*

$$\sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{k} \equiv -3q_p(3) \pmod p.$$

PROOF. By Theorem 4.3, we have

$$\begin{bmatrix} p \\ 0 \end{bmatrix}_3 (2) = 3^{p-1}.$$

By Lemma 2.3 (3), we have

$$\sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{k} = 3K_{p,3,0}(2) \equiv 3\frac{1 - \begin{bmatrix} p \\ 0 \end{bmatrix}_3 (2)}{p}$$
$$= 3\frac{1-3^{p-1}}{p} = -3q_p(3) \pmod p.$$ □

COROLLARY 4.3. *Let $p > 3$ be an odd prime. Then we have*

$$\sum_{k=1}^{[\frac{p+1}{3}]} \frac{(-8)^k}{12k-8} + \sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{6k-2} \equiv \left(\frac{-3}{p}\right)(2q_p(2) - q_p(3)) \pmod{p}.$$

PROOF. By Theorem 4.3,

$$\begin{bmatrix} p \\ 1 \end{bmatrix}_3 (2) = 3^{p-1} + (-3)^{\frac{p-1}{2}}, \quad \begin{bmatrix} p \\ 2 \end{bmatrix}_3 (2) = 3^{p-1} - (-3)^{\frac{p-1}{2}}.$$

Then

$$\begin{bmatrix} p \\ 1 \end{bmatrix}_3 (2) - \begin{bmatrix} p \\ 2 \end{bmatrix}_3 (2) = 2 \cdot (-3)^{\frac{p-1}{2}}.$$

By Lemmas 2.3 and 2.4, we have

$$\begin{aligned} &\sum_{k=1}^{[\frac{p+1}{3}]} \frac{(-8)^k}{12k-8} + \sum_{k=1}^{[\frac{p}{3}]} \frac{(-8)^k}{6k-2} = K_{p,3,1}(2) - K_{p,3,2}(2) \\ &\equiv \frac{2^p \cdot \left(\frac{-3}{p}\right) - 2 \cdot (-3)^{\frac{p-1}{2}}}{p} \\ &= \left(\frac{-3}{p}\right) \frac{(2^p - 2) + \left(2 - 2(-3)^{\frac{p-1}{2}} \left(\frac{-3}{p}\right)\right)}{p} \\ &\equiv \left(\frac{-3}{p}\right)(2q_p(2) - q_p(-3)) \pmod{p}. \end{aligned}$$

□

4.3. Further Results

LEMMA 4.1. *Let p be an odd prime with $p \nmid 3a(2-a)(a^2-a+1)$, and let $\{v_n\}_{n\geq 0}$ be the Lucas sequence defined as*

$$v_0 = 2, v_1 = 2 - a, v_{n+1} = (2-a)v_n - (a^2 - a + 1)v_{n-1} \text{ for } n \geq 1.$$

Then we have

$$\frac{v_p - (2-a)}{p} \equiv -\sum_{k=1}^{[\frac{p}{3}]} \frac{(-a)^{3k}}{k} - (a+1)q_p(a+1) \pmod{p}.$$

PROOF. Let $\{u_n\}_{n\geq 0}$ be the Lucas sequence defined as

$$u_0 = 0, u_1 = 1, u_{n+1} = (2-a)u_n - (a^2 - a + 1)u_{n-1} \text{ for } n \geq 1.$$

By Lemmas 2.1 and 2.2, we have $v_p = (2-a)u_p - 2(a^2-a+1)u_{p-1} = 2u_{p+1} - (2-a)u_p \equiv 2 - a \pmod p$. By Remark 4.1 and Lemma 2.3, we have $v_p = \Delta_3(0,p) = 3\begin{bmatrix} p \\ 0 \end{bmatrix}_3 (a) - (1+a)^p \equiv 3 - 3pK_{p,3,0}(a) - (1+a)^p \pmod{p^2}$. Thus

$$\frac{v_p - (2-a)}{p} \equiv -\sum_{k=1}^{[\frac{p}{3}]} \frac{(-a)^{3k}}{k} - (a+1)q_p(a+1) \pmod p. \qquad \square$$

In Theorem 4.2, when we express the Lucas quotient, it involves two K's, i.e., two sums. The following theorem can reduce the Lucas quotient to one sum.

THEOREM 4.4. *Let p be an odd prime with $p \nmid 3a(2-a)(a^3+1)$, and let $\{u_n\}_{n\geq 0}$ be the Lucas sequence defined as*

$$u_0 = 0, u_1 = 1, u_{n+1} = (2-a)u_n - (a^2 - a + 1)u_{n-1} \text{ for } n \geq 1.$$

Then we have, if $p \equiv 1 \pmod 3$,

$$\frac{u_{p-1}}{p} \equiv \frac{2}{3a^2} \sum_{k=1}^{\frac{p-1}{3}} \frac{(-a)^{3k}}{k} + \frac{1}{3a^2}\Big((2-a)q_p(a^2-a+1) + 2(a+1)q_p(a+1)\Big) \pmod p;$$

if $p \equiv 2 \pmod 3$,

$$\frac{u_{p+1}}{p} \equiv -\frac{2(a^2-a+1)}{3a^2} \sum_{k=1}^{\frac{p-2}{3}} \frac{(-a)^{3k}}{k} - \frac{a^2-a+1}{3a^2}\Big((2-a)q_p(a^2-a+1) + 2(a+1)q_p(a+1)\Big) \pmod p.$$

PROOF. Let $\{v_n\}_{n\geq 0}$ be the sequence as in Lemma 4.1. If $p \equiv 1 \pmod 3$, by Lemma 2.1, we have $u_{p-1} = \frac{1}{3a^2}((2-a)v_{p-1} - 2v_p)$. Thus

$$\frac{u_{p-1}}{p} = \frac{1}{3a^2}\left(\frac{(2-a)(v_{p-1}-2)}{p} - 2\frac{v_p - (2-a)}{p}\right).$$

If $p \equiv 2 \pmod 3$, by Lemma 2.1, we have $u_{p+1} = \frac{1}{3a^2}(2(a^2-a+1)v_p - (2-a)v_{p+1})$. Thus

$$\frac{u_{p+1}}{p} = \frac{1}{3a^2}\left(\frac{2(a^2-a+1)(v_p-(2-a))}{p} - \frac{(2-a)(v_{p+1}-2(a^2-a+1))}{p}\right).$$

Thus by Lemmas 2.5 and 4.1, we can prove this theorem. □

Given a value of a, by Theorem 4.4, we can obtain a concrete congruence for a specific Lucas quotient. We provide one such example.

COROLLARY 4.4. *Let $p \neq 3,7$ be an odd prime, and $\{u_n\}_{n\geq 0}$ be the Lucas sequence defined as*

$$u_0 = 0, u_1 = 1, u_{n+1} = 4u_n - 7u_{n-1} \text{ for } n \geq 1.$$

Then we have, if $p \equiv 1 \pmod 3$,

$$\frac{u_{p-1}}{p} \equiv \frac{1}{6}\sum_{k=1}^{\frac{p-1}{3}} \frac{8^k}{k} + \frac{1}{3}q_p(7) \pmod p;$$

if $p \equiv 2 \pmod 3$,

$$\frac{u_{p+1}}{p} \equiv -\frac{7}{6}\sum_{k=1}^{\frac{p-2}{3}} \frac{8^k}{k} - \frac{7}{3}q_p(7) \pmod p.$$

PROOF. Set $a = -2$ in Theorem 4.4. □

5. $\Delta_4(r, n)$ and Related Lucas Quotients

In this section, we consider the calculation of $\Delta_4(r, n)$.

5.1. General Properties

THEOREM 5.1. *Let $\{u_n\}_{n\geq 0}$ be the Lucas sequence defined as*

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = 2u_n - (a^2+1)u_{n-1} \text{ for } n \geq 1.$$

Then we have, for $n \geq 1$,

$$\begin{aligned}
\Delta_4(0,n) &= 2u_n - 2(a^2+1)u_{n-1} = 2u_{n+1} - 2u_n,\\
\Delta_4(1,n) &= 2au_n,\\
\Delta_4(2,n) &= -2u_n + 2(a^2+1)u_{n-1} = -2u_{n+1} + 2u_n,\\
\Delta_4(3,n) &= -2au_n.
\end{aligned}$$

PROOF. Since $u_{n+1} = 2u_n - (a^2+1)u_{n-1}$ for $n \geq 1$, we have $2u_{n+1} - 2u_n = 2u_n - 2(a^2+1)u_{n-1}$. It is easy to see that $\Delta_4(r,n) + \Delta_4(r+2,n) = 2\Delta_2(r,n) = 0$ for $n \geq 1$. So we need only consider $\Delta_4(0,n)$ and $\Delta_4(1,n)$.

Since $u_2 = 2$, one can verify the following simple facts:

$$\begin{aligned}
\Delta_4(0,1) &= 2 = 2u_1 - 2(a^2+1)u_0,\\
\Delta_4(0,2) &= -2a^2 + 2 = 2u_2 - 2(a^2+1)u_1,\\
\Delta_4(1,1) &= 2a = 2au_1,\\
\Delta_4(1,2) &= 4a = 2au_2.
\end{aligned}$$

By Theorem 3.2, for $n \geq 1$,

$$\Delta_4(r,n+2) = 2\Delta_4(r,n+1) - (a^2+1)\Delta_4(r,n).$$

Then we can prove the theorem by induction on n. □

THEOREM 5.2. *Let* $p \nmid a(a^4-1)$ *be an odd prime,* $\{u_n\}_{n\geq 0}$ *as in Theorem* 5.1, *and* $K_{p,4,r}(a)$ *as in Definition* 2.1. *Then we have*

$$\begin{aligned}
\frac{u_{p-1}}{p} \equiv{}& \frac{2}{a(a^2+1)}(aK_{p,4,0}(a) - K_{p,4,1}(a)) + \frac{2}{a^2+1}q_p(a)\\
&+ \frac{a^2-1}{2a(a^2+1)}(q_p(a+1) - q_p(a-1)) \pmod p, \text{ if } p \equiv 1 \pmod 4;
\end{aligned}$$

$$\begin{aligned}
\frac{u_{p+1}}{p} \equiv{}& -\frac{2}{a}(aK_{p,4,0}(a) + K_{p,4,1}(a)) - \frac{(a+1)^2}{2a}q_p(a+1)\\
&+ \frac{(a-1)^2}{2a}q_p(a-1) \pmod p, \text{ if } p \equiv 3 \pmod 4.
\end{aligned}$$

PROOF. Since $2^2 - 4(a^2+1) = -4a^2$, by Lemma 2.2, we have

$$p \mid u_{p-(\frac{-1}{p})}.$$

By Theorem 5.1, we have

$$\Delta_4(1,p) - a\Delta_4(0,p) = 2a(a^2+1)u_{p-1}, \tag{4}$$

and

$$\Delta_4(1,p) + a\Delta_4(0,p) = 2au_{p+1}. \tag{5}$$

Then, by Lemma 2.3(3), if $p \equiv 1 \pmod 4$, we have

$$\begin{aligned}\Delta_4(0,p) &\equiv 4 - 4pK_{p,4,0}(a) - (1+a)^p - (1-a)^p \pmod{p^2},\\ \Delta_4(1,p) &\equiv 4a^p - 4pK_{p,4,1}(a) - (1+a)^p + (1-a)^p \pmod{p^2}.\end{aligned}$$

Thus, by Eq.(4), we have

$$\begin{aligned}2a(a^2+1)u_{p-1} \equiv\ & 4p(aK_{p,4,0}(a) - K_{p,4,1}(a)) + 4a(a^{p-1}-1)\\ &+ (a^2-1)\left[(a+1)^{p-1} - (a-1)^{p-1}\right] \pmod{p^2}.\end{aligned}$$

Hence

$$\begin{aligned}\frac{u_{p-1}}{p} \equiv\ & \frac{2}{a(a^2+1)}(aK_{p,4,0}(a) - K_{p,4,1}(a)) + \frac{2}{a^2+1}q_p(a)\\ &+ \frac{a^2-1}{2a(a^2+1)}(q_p(a+1) - q_p(a-1)) \pmod p.\end{aligned}$$

If $p \equiv 3 \pmod 4$, by Lemma 2.3(3), we have

$$\Delta_4(0,p) \equiv 4 - 4pK_{p,4,0}(a) - (1+a)^p - (1-a)^p \pmod{p^2},$$

$$\Delta_4(1,p) \equiv -4pK_{p,4,1}(a) - (1+a)^p + (1-a)^p \pmod{p^2}.$$

Thus, by Eq.(5), we have

$$\begin{aligned}2au_{p+1} \equiv\ & -4p(aK_{p,4,0}(a) + K_{p,4,1}(a)) - (a+1)^2((a+1)^{p-1}-1)\\ &+ (a-1)^2((a-1)^{p-1}-1) \pmod{p^2}.\end{aligned}$$

Hence

$$\frac{u_{p+1}}{p} \equiv -\frac{2}{a}(aK_{p,4,0}(a) + K_{p,4,1}(a)) - \frac{(a+1)^2}{2a} q_p(a+1) + \frac{(a-1)^2}{2a} q_p(a-1) \pmod p. \qquad \square$$

Given a value of a, by Theorem 5.2, we can obtain a concrete congruence for a specific Lucas quotient. We provide one such example.

COROLLARY 5.5. *Let $p > 5$ be an odd prime, and $\{u_n\}_{n\geq 0}$ be the Lucas sequence defined as*

$$u_0 = 0,\ u_1 = 1,\ u_{n+1} = 2u_n - 5u_{n-1} \text{ for } n \geq 1.$$

Then, if $p \equiv 1 \pmod 4$,

$$\frac{u_{p-1}}{p} \equiv \frac{1}{10} \sum_{k=1}^{\frac{p-1}{4}} \frac{16^k}{k} + \frac{1}{40} \sum_{k=1}^{\frac{p-1}{4}} \frac{16^k}{4k-3} + \frac{2}{5} q_p(2) + \frac{3}{20} q_p(3) \pmod p;$$

if $p \equiv 3 \pmod 4$,

$$\frac{u_{p+1}}{p} \equiv \frac{1}{8} \sum_{k=1}^{\frac{p+1}{4}} \frac{16^k}{4k-3} - \frac{1}{2} \sum_{k=1}^{\frac{p-3}{4}} \frac{16^k}{k} - \frac{9}{4} q_p(3) \pmod p.$$

PROOF. Set $a = -2$ in Theorem 5.2. $\square$

5.2. Further Results

In Theorem 5.2, when we express the Lucas quotient, it involves two K's, i.e., two sums. The following theorem can reduce the Lucas quotient to one sum.

THEOREM 5.3. *With notation as in Theorem 5.2. Let $p \nmid a(a^4-1)$ be an odd prime. We have: if $p \equiv 1 \pmod 4$, then*

$$\begin{aligned}\frac{u_{p-1}}{p} \equiv& \frac{1}{2a^2}\left(\sum_{k=1}^{\frac{p-1}{4}} \frac{a^{4k}}{k} + (1+a)q_p(1+a) + (1-a)q_p(1-a) + q_p(a^2+1)\right)\\ \equiv& \frac{1}{2a}\left(-4\sum_{k=1}^{\frac{p-1}{4}} \frac{a^{4k-1}}{4k-1} + (1+a)q_p(1+a) - (1-a)q_p(1-a)\right)\\ &- \frac{1}{2}q_p(a^2+1) \pmod p;\end{aligned}$$

if $p \equiv 3 \pmod 4$, *then*

$$\frac{u_{p+1}}{p} \equiv -\frac{a^2+1}{2a^2}\left(\sum_{k=1}^{\frac{p-3}{4}}\frac{a^{4k}}{k} + (1+a)q_p(1+a) + (1-a)q_p(1-a) + q_p(a^2+1)\right)$$

$$\equiv \frac{a^2+1}{2a}\left(4\sum_{k=1}^{\frac{p+1}{4}}\frac{a^{4k-3}}{4k-3} - (1+a)q_p(1+a) + (1-a)q_p(1-a)\right)$$

$$+ \frac{a^2+1}{2}q_p(a^2+1) \pmod p.$$

PROOF. Let $\{v_n\}_{n\geq 0}$ be the Lucas sequence defined as

$$v_0 = 2, v_1 = 2, v_{n+1} = 2v_n - (a^2+1)v_{n-1} \text{ for } n \geq 1.$$

By Lemmas 2.1 and 2.2, we have $v_p = 2u_p - 2(a^2+1)u_{p-1} = 2u_{p+1} - 2u_p \equiv 2 \pmod p$. By Theorem 5.1 and Lemma 2.1, we have $\Delta_4(0,p) = 2u_{p+1} - 2u_p = v_p$. By Lemma 2.3, we have

$$\Delta_4(0,p) = 4\begin{bmatrix} p \\ 0 \end{bmatrix}_4 (a) - (1+a)^p - (1-a)^p$$

$$\equiv 4 - 4pK_{p,4,0}(a) - (1+a)^p - (1-a)^p \pmod{p^2}.$$

Thus

$$\frac{v_p - 2}{p} \equiv -\sum_{k=1}^{[\frac{p}{4}]}\frac{a^{4k}}{k} - (1+a)q_p(1+a) - (1-a)q_p(1-a) \pmod p. \quad (6)$$

If $p \equiv 1 \pmod 4$, by Theorem 5.1 and Lemma 2.3 we have $-2au_p = \Delta_4(3,p)$ $= 4\begin{bmatrix} p \\ 3 \end{bmatrix}_4 (a) - (1+a)^p + (1-a)^p \equiv -4pK_{p,4,3}(a) - (1+a)^p + (1-a)^p \pmod{p^2}$. So we have

$$\frac{u_p - 1}{p} \equiv \frac{1}{2a}\left(4K_{p,4,3}(a) + (1+a)q_p(1+a) - (1-a)q_p(1-a)\right) \pmod p. \quad (7)$$

By Lemma 2.1, we have $u_{p-1} = \frac{1}{-4a^2}(2v_p - 2v_{p-1}) = \frac{1}{2a^2}(v_{p-1} - v_p)$ and $u_{p-1} = u_p - \frac{1}{2}v_{p-1}$. By Lemma 2.5 and Eq.(6), we have

$$\begin{aligned}\frac{u_{p-1}}{p} &= \frac{1}{2a^2}\left(\frac{v_{p-1}-2}{p} - \frac{v_p - 2}{p}\right)\\ &\equiv \frac{1}{2a^2}\left(\sum_{k=1}^{\frac{p-1}{4}} \frac{a^{4k}}{k} + (1+a)q_p(1+a) + (1-a)q_p(1-a) + q_p(a^2+1)\right) \pmod p.\end{aligned}$$

Similarly, by Lemma 2.5 and Eq.(7), we have

$$\begin{aligned}\frac{u_{p-1}}{p} =& \frac{u_p - 1}{p} - \frac{1}{2}\frac{v_{p-1}-2}{p}\\ \equiv& \frac{1}{2a}\left(-4\sum_{k=1}^{\frac{p-1}{4}} \frac{a^{4k-1}}{4k-1} + (1+a)q_p(1+a) - (1-a)q_p(1-a)\right)\\ &- \frac{1}{2}q_p(a^2+1) \pmod p.\end{aligned}$$

If $p \equiv 3 \pmod 4$, by Theorem 5.1 and Lemma 2.3 we have $2au_p = \Delta_4(1,p) = 4\begin{bmatrix} p \\ 1 \end{bmatrix}_4 (a) - (1+a)^p + (1-a)^p \equiv -4pK_{p,4,1}(a) - (1+a)^p + (1-a)^p \pmod{p^2}$. So we have

$$\frac{u_p+1}{p} \equiv \frac{1}{2a}\left(-4K_{p,4,1}(a) - (1+a)q_p(1+a) + (1-a)q_p(1-a)\right) \pmod p. \quad (8)$$

By Lemma 2.1, we have $u_{p+1} = \frac{1}{-4a^2}(2v_{p+1} - 2(a^2+1)v_p) = \frac{1}{2a^2}((a^2+1)v_p - v_{p+1})$ and $u_{p+1} = (a^2+1)u_p + \frac{1}{2}v_{p+1}$. By Lemma 2.5 and Eq.(6), we have

$$\begin{aligned}&\frac{u_{p+1}}{p} = \frac{1}{2a^2}\left((a^2+1)\frac{v_p - 2}{p} - \frac{v_{p+1} - 2(a^2+1)}{p}\right)\\ &\equiv -\frac{a^2+1}{2a^2}\left(\sum_{k=1}^{\frac{p-3}{4}} \frac{a^{4k}}{k} + (1+a)q_p(1+a) + (1-a)q_p(1-a)\right)\\ &-\frac{a^2+1}{2a^2}q_p(a^2+1) \pmod p.\end{aligned}$$

Similarly, by Lemma 2.5 and Eq.(8), we have

$$\begin{aligned}\frac{u_{p+1}}{p} =&(a^2+1)\frac{u_p+1}{p}+\frac{1}{2}\frac{v_{p+1}-2(a^2+1)}{p}\\ \equiv&\frac{a^2+1}{2a}\left(4\sum_{k=1}^{\frac{p+1}{4}}\frac{a^{4k-3}}{4k-3}-(1+a)q_p(1+a)+(1-a)q_p(1-a)\right)\\ &+\frac{a^2+1}{2}q_p(a^2+1)\pmod p.\end{aligned}$$

□

Given a value of a, by Theorem 5.3, we can obtain a concrete congruence for a specific Lucas quotient. We provide one such example.

COROLLARY 5.6. *Let $p>5$ be an odd prime, and $\{u_n\}_{n\geq 0}$ be the Lucas sequence defined as*

$$u_0=0, u_1=1, u_{n+1}=2u_n-5u_{n-1} \text{ for } n\geq 1.$$

Then we have: *if* $p\equiv 1 \pmod 4$,

$$\begin{aligned}\frac{u_{p-1}}{p} \equiv&\frac{1}{8}\sum_{k=1}^{\frac{p-1}{4}}\frac{16^k}{k}+\frac{3}{8}q_p(3)+\frac{1}{8}q_p(5)\\ \equiv&-\frac{1}{2}\sum_{k=1}^{\frac{p-1}{4}}\frac{16^k}{4k-1}+\frac{3}{4}q_p(3)-\frac{1}{2}q_p(5)\pmod p;\end{aligned}$$

if $p\equiv 3 \pmod 4$,

$$\begin{aligned}\frac{u_{p+1}}{p} \equiv&-\frac{5}{8}\sum_{k=1}^{\frac{p-3}{4}}\frac{16^k}{k}-\frac{15}{8}q_p(3)-\frac{5}{8}q_p(5)\\ \equiv&\frac{5}{8}\sum_{k=1}^{\frac{p+1}{4}}\frac{16^k}{4k-3}-\frac{15}{4}q_p(3)+\frac{5}{2}q_p(5)\pmod p.\end{aligned}$$

PROOF. Set $a=-2$ in Theorem 5.3. □

6. $\Delta_6(r,n)$

In this section, we consider the calculation of $\Delta_6(r,n)$.

THEOREM 6.1. *Let* $\{V_n\}_{n\geq 0}$ *be the Lucas sequences defined as*

$$V_0 = 2,\ V_1 = a+2,\ V_{n+1} = (a+2)V_n - (a^2+a+1)V_{n-1} \text{ for } n \geq 1.$$

Let $\{v_n\}_{n\geq 0}$ *be the Lucas sequences defined as*

$$v_0 = 2,\ v_1 = 2-a,\ v_{n+1} = (2-a)v_n - (a^2-a+1)v_{n-1} \text{ for } n \geq 1.$$

Then we have, for $n \geq 1$,

$$\begin{aligned}
\Delta_6(0,n) &= V_n + v_n,\\
\Delta_6(1,n) &= -\frac{1}{a}V_n + \frac{a^2+a+1}{a}V_{n-1} - \frac{1}{a}v_n + \frac{a^2-a+1}{a}v_{n-1},\\
\Delta_6(2,n) &= -\frac{a+1}{a}V_n + \frac{a^2+a+1}{a}V_{n-1} - \frac{a-1}{a}v_n - \frac{a^2-a+1}{a}v_{n-1},\\
\Delta_6(3,n) &= -V_n + v_n,\\
\Delta_6(4,n) &= \frac{1}{a}V_n - \frac{a^2+a+1}{a}V_{n-1} - \frac{1}{a}v_n + \frac{a^2-a+1}{a}v_{n-1},\\
\Delta_6(5,n) &= \frac{a+1}{a}V_n - \frac{a^2+a+1}{a}V_{n-1} - \frac{a-1}{a}v_n - \frac{a^2-a+1}{a}v_{n-1}.
\end{aligned}$$

PROOF. Since $V_2 = -a^2+2a+2$, $v_2 = -a^2-2a+2$, $V_3 = -2a^3-3a^2+3a+2$, $v_3 = 2a^3-3a^2-3a+2$, $V_4 = -a^4-8a^3-6a^2+4a+2$, $v_4 = -a^4+8a^3-6a^2-4a+2$, one can verify the following simple facts:

$$\begin{aligned}
\Delta_6(0,1) &= 4 = V_1 + v_1,\\
\Delta_6(0,2) &= -2a^2+4 = V_2 + v_2,\\
\Delta_6(0,3) &= -6a^2+4 = V_3 + v_3,\\
\Delta_6(0,4) &= -2a^4 - 12a^2 + 4 = V_4 + v_4;\\
\Delta_6(1,1) &= 4a = -\frac{1}{a}V_1 + \frac{a^2+a+1}{a}V_0 - \frac{1}{a}v_1 + \frac{a^2-a+1}{a}v_0,\\
\Delta_6(1,2) &= 8a = -\frac{1}{a}V_2 + \frac{a^2+a+1}{a}V_1 - \frac{1}{a}v_2 + \frac{a^2-a+1}{a}v_1,\\
\Delta_6(1,3) &= -2a^3+12a = -\frac{1}{a}V_3 + \frac{a^2+a+1}{a}V_2 - \frac{1}{a}v_3 + \frac{a^2-a+1}{a}v_2,\\
\Delta_6(1,4) &= -8a^3+16a = -\frac{1}{a}V_4 + \frac{a^2+a+1}{a}V_3 - \frac{1}{a}v_4 + \frac{a^2-a+1}{a}v_3.
\end{aligned}$$

By Theorem 3.2, we have, for $n \geq 1$,

$$\begin{aligned}\Delta_6(r, n+4) =& 4\Delta_6(r, n+3) - (a^2+6)\Delta_6(r, n+2) \\ &+ (2a^2+4)\Delta_6(r, n+1) - (a^4+a^2+1)\Delta_6(r, n).\end{aligned}$$

Thus we can prove the theorem by induction on n for $r = 0,1$.

It is easy to see that $\Delta_6(r, n) + \Delta_6(r+2, n) + \Delta_6(r+4, n) = 3\Delta_2(r, n) = 0$ and $\Delta_6(r, n) + \Delta_6(r+3, n) = 2\Delta_3(r, n)$. Hence $\Delta_6(2, n) = -\Delta_6(0, n) - \Delta_6(4, n) = -\Delta_6(0, n) + \Delta_6(1, n) - 2\Delta_3(1, n)$. Thus, by Remark 4.1 and the formulae for $\Delta_6(0, n)$ and $\Delta_6(1, n)$, we can obtain the formula for $\Delta_6(2, n)$. Finally, by Remark 4.1 and the formulae for $\Delta_6(0, n)$, $\Delta_6(1, n)$ and $\Delta_6(2, n)$, we can obtain the formulae for $\Delta_6(3, n)$, $\Delta_6(4, n)$ and $\Delta_6(5, n)$. □

Note that, for $m = 6$, since the Lucas sequences in Theorem 6.1 have already appeared in Theorem 4.1, we can not obtain any new Lucas quotient.

Acknowledgments

The work of this paper was supported by the NNSF of China (Grant No. 11471314), and the National Center for Mathematics and Interdisciplinary Sciences, CAS.

Bibliography

1. ***R. Crandall and C. Pomerance,*** *Prime Numbers*, *A Computational Perspective* (second edition), Springer, New York, 2005.
2. ***Y. Deng and Y. Pan,*** *The Sum of Binomial Coefficients and Integer Factorization*, Integers, **16** (2016), Paper No. A42, 18 p.
3. ***R. L. Rivest, A. Shamir and L. Adleman,*** *A Method for Obtaining Digital Signatures and Public-key Cryptosystems*, Comm. ACM, **21** (1978), 120–126.
4. ***Z.-H. Sun,*** *Combinatorial Sum* $\sum_{k=0,\ k\equiv r \pmod m}^{n} \binom{n}{k}$ *and its Applications in Number Theory* (I), Nanjing Daxue Xuebao Shuxue Bannian Kan, **9** (1992), 227–240.
5. ***Z.-H. Sun,*** *Combinatorial Sum* $\sum_{k=0,k\equiv r \pmod m}^{n} \binom{n}{k}$ *and its Applications in Number Theory* (II), Nanjing Daxue Xuebao Shuxue Bannian Kan, **10** (1993), 105–118.
6. ***Z.-H. Sun,*** *Combinatorial Sum* $\sum_{k=0,k\equiv r \pmod m}^{n} \binom{n}{k}$ *and its Applications in Number Theory* (III), Nanjing Daxue Xuebao Shuxue Bannian Kan, **12** (1995), 90–102.
7. ***Z.-H. Sun and Z.-W. Sun,*** *Fibonacci Numbers and Fermat's Last Theorem*, Acta Arith., **60** (1992), 371–388.

8. ***Z.-W. Sun,*** *A Congruence for Primes*, Proc. Amer. Math. Soc., **123**(1995), 1341–1346.
9. ***Z.-W. Sun,*** *On the Sum* $\sum_{k\equiv r \pmod m} \binom{n}{k}$ *and Related Congruences*, Israel J. Math., **128** (2002), 135–156.
10. ***D. D. Wall,*** *Fibonacci Series Modulo* m, Amer. Math. Monthly, **67** (1960), 525–532.
11. ***H. C. Williams,*** *A Note on the Fibonacci Quotient* $F_{p-\varepsilon}/p$, Canad. Math. Bull, **25** (1982), 366–370.

JIANGSHUAI YANG

Key Laboratory
of Mathematics
Mechanization, NCMIS,
Academy of Mathematics
and Systems
Science, Chinese Academy
of Sciences,
Beijing 100190,
People's Republic of China
yangjiangshuai@amss.ac.cn

YINGPU DENG

Key Laboratory
of Mathematics
Mechanization, NCMIS,
Academy of Mathematics
and Systems
Science, Chinese Academy
of Sciences,
Beijing 100190,
People's Republic of China
School of Mathematical
Sciences,
University of Chinese
Academy of Sciences, Beijing
100049, People's Republic
of China
dengyp@amss.ac.cn