PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 129, Number 12, Pages 3471–3478
S 0002-9939(01)06234-7
Article electronically published on June 8, 2001

AN EXTENSION OF LUCAS' THEOREM

HONG HU AND ZHI-WEI SUN

(Communicated by David E. Rohrlich)

ABSTRACT. Let p be a prime. A famous theorem of Lucas states that $\binom{mp+s}{np+t} \equiv \binom{m}{n}\binom{s}{t} \pmod{p}$ if m, n, s, t are nonnegative integers with $s, t < p$. In this paper we aim to prove a similar result for generalized binomial coefficients defined in terms of second order recurrent sequences with initial values 0 and 1.

1. INTRODUCTION

Let $\mathbb{N} = \{0, 1, 2, \cdots\}$, $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$ and $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Fix $A, B \in \mathbb{Z}^*$. The Lucas sequence $\{u_n\}_{n\in\mathbb{N}}$ is defined as follows:

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

Its companion sequence $\{v_n\}_{n\in\mathbb{N}}$ is given by

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

By induction, for $n = 0, 1, 2, \cdots$ we have

$$u_n = \sum_{0\le k<n} \alpha^k \beta^{n-1-k} \quad \text{and} \quad v_n = \alpha^n + \beta^n$$

where

$$\alpha = \frac{A + \sqrt{\Delta}}{2},\ \beta = \frac{A - \sqrt{\Delta}}{2} \text{ and } \Delta = A^2 - 4B.$$

It follows that

$$v_n = 2u_{n+1} - Au_n,\ u_{2n} = u_n v_n \text{ and } v_{2n} = v_n^2 - 2B^n \quad \text{for } n \in \mathbb{N}.$$

For $a, b \in \mathbb{Z}$ let (a, b) denote the greatest common divisor of a and b. A nice result of E. Lucas asserts that if $(A, B) = 1$, then $(u_m, u_n) = |u_{(m,n)}|$ for $m, n \in \mathbb{N}$ (cf. L. E. Dickson [1]).

In the case $A^2 = B = 1$, by induction on $n \in \mathbb{N}$ we find that $u_n = 0$ if $3 \mid n$, and

$$u_n = \begin{cases} 1 & \text{if } A = -1 \ \&\ 3 \mid n - 1, \text{ or } A = 1 \ \&\ n \equiv 1, 2 \pmod{6}; \\ -1 & \text{if } A = -1 \ \&\ 3 \mid n + 1, \text{ or } A = 1 \ \&\ n \equiv -1, -2 \pmod{6}. \end{cases}$$

Received by the editors April 18, 2000.

2000 *Mathematics Subject Classification.* Primary 11B39; Secondary 11A07, 11B65.

The second author is responsible for all the communications, and supported by the Teaching and Research Award Program for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of P. R. China.

We set $[n]=\prod_{0<k\le n}u_k$ for $n\in\mathbb{N}$, and regard an empty product as value 1. For $n,k\in\mathbb{N}$ with $[n]\ne 0$, we define the Lucas u-nomial coefficient $\left[{n \atop k}\right]$ as follows:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{cases} \frac{[n]}{[k][n-k]} & \text{if } n\ge k, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

In the case $A=2$ and $B=1$, $\left[{n \atop k}\right]$ is exactly the binomial coefficient $\binom{n}{k}$; when $A=q+1$ and $B=q$ where $q\in\mathbb{Z}$ and $|q|>1$, $\left[{n \atop k}\right]$ coincides with Gaussian q-nomial coefficient $\binom{n}{k}_q$ because $u_j=(q^j-1)/(q-1)$ for $j=0,1,2,\cdots$. For generalized binomial coefficients formed from an arbitrary sequence of positive integers, the reader is referred to the elegant paper of D. E. Knuth and H. S. Wilf [5].

Let $d>1$ and $q>0$ be integers with $d\mid u_q$. If $(A,B)=1$ and $d\nmid u_k$ for $k=1,\cdots,q-1$, then for any $n\in\mathbb{N}$ we have

$$d\mid u_n \iff d \text{ divides } (u_n,u_q)=|u_{(n,q)}| \iff q=(n,q) \iff q\mid n;$$

this property is usually called the *regular divisibility* of $\{u_n\}_{n\in\mathbb{N}}$. If $(d,u_k)=1$ for all $0<k<q$, then we write $q=d_*$ and call d a *primitive divisor* of u_q while q is called the *rank of apparition* of d. When $(A,B)=1$, $q=d_*$, $n\in\mathbb{N}$ and $q\nmid n$, we have

$$(d,u_n)=((d,u_q),u_n)=(d,(u_n,u_q))=(d,u_{(n,q)})=1.$$

When p is an odd prime not dividing B, p_* exists because $p\mid u_{p-(\frac{\Delta}{p})}$ as is well known where $(-)$ denotes the Legendre symbol. On the other hand, drawing upon some ideas of A. Schinzel [6], C. L. Stewart [7] proved in 1977 that if A is prime to B and α/β is not a root of unity, then u_n has a primitive prime divisor for each $n>e^{452}2^{67}$; P. M. Voutier [9] conjectured in 1995 that the lower bound $e^{452}2^{67}$ can be replaced by 30.

For $m\in\mathbb{Z}$ we use $\mathbb{Z}_m$ to denote the ring of rationals in the form a/b with $a\in\mathbb{Z},\ b\in\mathbb{Z}^+$ and $(b,m)=1$. When $r\in\mathbb{Z}_m$, by $x\equiv r \pmod m$ we mean that x can be written as $r+my$ with $y\in\mathbb{Z}_m$.

For convenience we set $R(q)=\{x\in\mathbb{Z}:\ 0\le x<q\}$ for $q\in\mathbb{Z}^+$.

Our main result is as follows.

Theorem. *Suppose that $(A,B)=1$, and $A\ne\pm1$ or $B\ne1$. Then $u_k\ne0$ for every $k=1,2,3,\cdots$. Let $q\in\mathbb{Z}^+$, $m,n\in\mathbb{N}$ and $s,t\in R(q)$. Then*

$$\begin{bmatrix} mq+s \\ nq+t \end{bmatrix} \equiv \binom{m}{n}\begin{bmatrix} s \\ t \end{bmatrix} u_{q+1}^{(nq+t)(m-n)+n(s-t)} \pmod{w_q} \tag{4}$$

where w_q is the largest divisor of u_q prime to $u_1,\cdots,u_{q-1}$. If q or $m(n+t)+n(s+1)$ is even, then

$$\begin{bmatrix} mq+s \\ nq+t \end{bmatrix} \equiv \binom{m}{n}\begin{bmatrix} s \\ t \end{bmatrix} (-1)^{(mt-ns)(q-1)}B^{\frac{q}{2}((nq+t)(m-n)+n(s-t))} \pmod{w_q}. \tag{5}$$

Remark 1. Providing $(A,B)=1$ and $q\in\mathbb{Z}^+$, $(u_q,\prod_{0<k<q}u_k)=1$ if and only if $u_d=\pm1$ for all proper divisors d of q (this is because $(u_q,u_k)=|u_{(q,k)}|$); therefore u_q is prime to $u_1,\cdots,u_{q-1}$ if q is a prime.

When $A=2$ and $B=1$, we have $u_k=k$ for all $k\in\mathbb{N}$, hence the Theorem yields Lucas' theorem which asserts that

$$\binom{mp+s}{np+t}\equiv\binom{m}{n}\binom{s}{t} \pmod p,$$

where p is a prime and m, n, s, t are nonnegative integers with $s, t < p$. In the case $A = a + 1$ and $B = a$ where $a \in \mathbb{Z}$ and $|a| > 1$, as $u_{q+1} = (a^{q+1} - 1)/(a - 1) = au_q + 1 \equiv 1 \pmod{u_q}$ for $q \in \mathbb{Z}^+$, our Theorem implies Theorem 3.11 of R. D. Fray [2].

Theorem 3 of B. Wilson [10] follows from our Theorem in the special case $A = 1,\ B = -1$ and $s \geq t$. Wilson used a result of Kummer concerning the highest power of a prime dividing a binomial coefficient; see Knuth and Wilf [5] for various generalizations of Kummer's theorem. Our proof of the Theorem is more direct; we don't use Kummer's theorem in any form.

Example. (i) Set $A = 4$ and $B = 1$. Then

$$u_0 = 0,\ u_1 = 1,\ u_2 = 4,\ u_3 = 15,\ u_4 = 56,\ u_5 = 209,\ u_6 = 780.$$

Clearly $p = 13$ is the largest primitive divisor of $u_6 = 780$. By the Theorem,

$$\begin{aligned}\begin{bmatrix}71\\25\end{bmatrix} = \begin{bmatrix}11\times 6+5\\4\times 6+1\end{bmatrix} \equiv &\binom{11}{4}\begin{bmatrix}5\\1\end{bmatrix}(-1)^{11\times 1-4\times 5} = 330\times u_5\times(-1)\\ \equiv &-330\times 209 \equiv -5\times 1 \equiv 8 \pmod{13}.\end{aligned}$$

(ii) Take $A = 1$ and $B = -7$. Then $w_3 = u_3 = 8$ and $u_4 = 15$. By the Theorem,

$$\begin{bmatrix}35\\10\end{bmatrix} = \begin{bmatrix}11\times 3+2\\3\times 3+1\end{bmatrix} \equiv \binom{11}{3}\begin{bmatrix}2\\1\end{bmatrix}15^{10(11-3)+3(2-1)} \equiv 3 \pmod{8}.$$

2. Several lemmas

Lemma 1. *Let n and k be positive integers with $n > k$ and $[n] \neq 0$. Then*

$$\begin{bmatrix}n\\k\end{bmatrix} = u_{k+1}\begin{bmatrix}n-1\\k\end{bmatrix} - Bu_{n-k-1}\begin{bmatrix}n-1\\k-1\end{bmatrix}. \tag{6}$$

If $2 \mid A$ and $2 \nmid B$, then $\left[{n \atop k}\right] \equiv \binom{n}{k} \pmod{2}$.

Proof. Clearly the right hand side of (6) coincides with

$$\begin{aligned}&u_{k+1}\frac{[n-1]}{[k][n-1-k]} - Bu_{n-k-1}\frac{[n-1]}{[k-1][n-k]}\\ =&\frac{[n-1]}{[k][n-k]}(u_{k+1}u_{n-k} - Bu_ku_{n-k-1}) = \begin{bmatrix}n\\k\end{bmatrix},\end{aligned}$$

where in the last step we use the identity $u_{k+1}u_l - Bu_ku_{l-1} = u_{k+l}$ which can be easily proved by induction on $l \in \mathbb{Z}^+$.

Now suppose that $2 \nmid (A-1)B$. Then $u_1, u_3, u_5, \cdots$ are odd and $u_2, u_4, u_6, \cdots$ are even. If

$$\begin{bmatrix}n-1\\k\end{bmatrix} \equiv \binom{n-1}{k} \pmod{2} \quad\text{and}\quad \begin{bmatrix}n-1\\k-1\end{bmatrix} \equiv \binom{n-1}{k-1} \pmod{2},$$

then (6) yields that

$$\begin{aligned}\begin{bmatrix}n\\k\end{bmatrix} \equiv&(k+1)\binom{n-1}{k} - (n-k-1)\binom{n-1}{k-1}\\ \equiv&(k+1)\binom{n}{k} - n\binom{n-1}{k-1} = \binom{n}{k} \pmod{2}.\end{aligned}$$

So $\left[{n \atop k}\right] \equiv \binom{n}{k} \pmod{2}$ by induction. □

Remark 2. In light of Lemma 1, by induction, if $n \in \mathbb{N}$ and $[n] \neq 0$, then $\left[{n \atop k} \right] \in \mathbb{Z}$ for all $k \in \mathbb{N}$. This was also realized by W. A. Kimball and W. A. Webb [4]. In 1989 Knuth and Wilf [5] proved that generalized binomial coefficients, formed from a regularly divisible sequence of positive integers, are always integral.

Lemma 2. *Let q be a positive integer. Then $u_{q+1}^2 \equiv B^q \pmod{u_q}$. If $2 \mid q$, then $u_{q+1} \equiv -B^{q/2} \pmod{d}$ for any primitive divisor d of u_q.*

Proof. As

$$\begin{pmatrix} u_q & u_{q-1} \\ u_{q+1} & u_q \end{pmatrix} = \begin{pmatrix} u_{q-1} & u_{q-2} \\ u_q & u_{q-1} \end{pmatrix} \begin{pmatrix} A & 1 \\ -B & 0 \end{pmatrix} = \cdots = \begin{pmatrix} u_1 & u_0 \\ u_2 & u_1 \end{pmatrix} \begin{pmatrix} A & 1 \\ -B & 0 \end{pmatrix}^{q-1},$$

we have $u_q^2 - u_{q-1}u_{q+1} = B^{q-1}$ and hence $u_{q+1}^2 \equiv -Bu_{q-1}u_{q+1} \equiv B^q \pmod{u_q}$.

Now assume that $q = 2n$ where $n \in \mathbb{Z}^+$. Let d be a primitive divisor of u_q. Since $u_n v_n = u_q \equiv 0 \pmod{d}$ and $(d, u_n) = 1$, we have $d \mid v_n$ and hence

$$u_{q+1} = \frac{Au_q + v_q}{2} = \frac{Au_n v_n + v_n^2 - 2B^n}{2} = u_{n+1}v_n - B^n \equiv -B^n \pmod{d}.$$

This ends the proof. □

Lemma 3. *Let $k, q \in \mathbb{Z}^+$. Then*

$$u_{kq+l} \equiv u_{q+1}^k u_l \pmod{u_q} \quad \text{for } l = 0, 1, 2, \cdots. \tag{7}$$

If $u_q \neq 0$, then

$$\frac{u_{kq}}{ku_q} \equiv u_{q+1}^{k-1} + (k-1)A\frac{u_q}{2} \pmod{u_q}. \tag{8}$$

Proof. Let $l \in \mathbb{N}$. By Lemma 2 of Z.-W. Sun [8],

$$u_{kq+l} = \sum_{r=0}^{k} \binom{k}{r} c^{k-r} u_q^r u_{l+r}$$

where $c = -Bu_{q-1} = u_{q+1} - Au_q$. Clearly $u_{kq+l} \equiv u_{q+1}^k u_l \pmod{u_q}$. In the case $u_q \neq 0$,

$$\frac{u_{kq}}{ku_q} = \sum_{r=1}^{k} \frac{1}{k}\binom{k}{r} c^{k-r} u_q^{r-1} u_r = \sum_{r=1}^{k} \binom{k-1}{r-1} \frac{u_q^{r-1}}{r} c^{k-r} u_r.$$

For any prime p and integer $r > 3$ we have

$$p^{r-2} \geq (1+1)^{r-2} \geq 1 + (r-2) + 1 = r,$$

therefore $u_q^{r-2}/r \in \mathbb{Z}_{u_q}$ for $r = 3, 4, \cdots$. If $2 \mid u_q$ and $2 \nmid A$, then $2 \nmid B$ (otherwise $u_q \equiv u_{q-1} \equiv \cdots \equiv u_1 \not\equiv 0 \pmod{2}$), as $u_{q+1}^2 \equiv B^q \pmod{u_q}$ we have $c \equiv u_{q+1} \equiv 1 \pmod{2}$. Thus (8) holds providing $u_q \neq 0$. □

Lemma 4. *Assume that $(A, B) = 1$, $q \in \mathbb{Z}^+$ and $u_k \neq 0$ for all $k \in \mathbb{Z}^+$. Then for any $m, n \in \mathbb{N}$ and $s, t \in R(q)$ we have*

$$\begin{bmatrix} mq + s \\ nq + t \end{bmatrix} \equiv \begin{bmatrix} mq \\ nq \end{bmatrix} \begin{bmatrix} s \\ t \end{bmatrix} u_{q+1}^{t(m-n)+n(s-t)} \pmod{w_q} \tag{9}$$

where w_q is the largest divisor of u_q prime to $u_1, \cdots, u_{q-1}$.

Proof. Let $m, n \in \mathbb{N}$ and $s, t \in R(q)$. If $m < n$, then $mq + s < (m+1)q \le nq + t$ and hence $\left[{mq+s \atop nq+t} \right] = 0 = \left[{mq \atop nq} \right]$. If $m = n$ and $s < t$, then $\left[{mq+s \atop nq+t} \right] = 0 = \left[{s \atop t} \right]$. Below we assume that $m \ge n$ and $mq + s \ge nq + t$.

As $(A, B) = 1$, $(u_q, u_{q+1}) = |u_{(q,q+1)}| = 1$. Observe that w_q is prime to $u_{q+1} \prod_{0<r<q} u_r$, and

$$\begin{bmatrix} mq+s \\ nq+t \end{bmatrix} = \frac{\prod_{(m-n)q<j\le mq} u_j}{\prod_{0<j\le nq} u_j} \times \frac{\prod_{0<r\le s} u_{mq+r}}{\prod_{0<r\le t} u_{nq+r}} \times \begin{cases} \prod_{0<r\le s-t} u^{-1}_{(m-n)q+r} & \text{if } s \ge t, \\ \prod_{0\le r<t-s} u_{(m-n)q-r} & \text{if } s < t. \end{cases}$$

By Lemma 3, $u_{kq+r} \equiv u^k_{q+1} u_r \pmod{w_q}$ for any $k, r \in \mathbb{N}$. So

$$\begin{aligned} \begin{bmatrix} mq+s \\ nq+t \end{bmatrix} &\equiv \begin{bmatrix} mq \\ nq \end{bmatrix} \times \frac{\prod_{0<r\le s}(u^m_{q+1}u_r)}{\prod_{0<r\le t}(u^n_{q+1}u_r)} \\ &\quad \times \begin{cases} \prod_{0<r\le s-t}(u^{n-m}_{q+1}u^{-1}_r) \pmod{w_q} & \text{if } s \ge t, \\ 0 \pmod{w_q} & \text{otherwise}, \end{cases} \\ &\equiv \begin{bmatrix} mq \\ nq \end{bmatrix} \frac{[s]}{[t]} u^{ms-nt}_{q+1} \times \begin{cases} u^{(n-m)(s-t)}_{q+1}/[s-t] \pmod{w_q} & \text{if } s \ge t, \\ 0 \pmod{w_q} & \text{if } s < t, \end{cases} \\ &\equiv \begin{bmatrix} mq \\ nq \end{bmatrix} \begin{bmatrix} s \\ t \end{bmatrix} u^{t(m-n)+n(s-t)}_{q+1} \pmod{w_q}. \end{aligned}$$

This concludes the proof. □

3. Proof of the Theorem

Let us first show that $u_1, u_2, u_3, \cdots$ are all nonzero.

If $\Delta = 0$, then $\alpha = \beta = A/2$ and hence

$$u_k = \sum_{0\le r<k} \alpha^r \beta^{k-1-r} = k \left(\frac{A}{2}\right)^{k-1} \ne 0 \quad \text{for } k = 1, 2, 3, \cdots .$$

Suppose that $u_k = 0$ for some $k \in \mathbb{Z}^+$. Then $\Delta \ne 0$, $\alpha \ne \beta$ and $\alpha^k = \beta^k$. Since the field $\mathbb{Q}(\sqrt{\Delta})$ contains the root $\alpha/\beta \ne \pm 1$ of unity, by Propositions 13.1.5 and 13.1.6 of K. Ireland and M. Rosen [3] there exists a positive integer D such that $\Delta = -D^2$ and $\alpha/\beta \in \{\pm i\}$, or $\Delta = -3D^2$ and $\alpha/\beta \in \{\pm\omega, \pm\omega^2\}$ where $\omega = (-1 + \sqrt{-3})/2$. In the former case, $(A + Di)/(A - Di) \in \{\pm i\}$; hence $A^2 = D^2$ and $2B = (A^2 - \Delta)/2 = D^2$. This is impossible since A or B is odd. Thus the latter case happens. Now that

$$\frac{A + D\sqrt{-3}}{A - D\sqrt{-3}} = \frac{A^2 - 3D^2 + 2AD\sqrt{-3}}{A^2 + 3D^2} \in \left\{ \frac{-1 \pm \sqrt{-3}}{2}, \frac{1 \pm \sqrt{-3}}{2} \right\},$$

we have $A^2 - 3D^2 = \pm 2AD$ and hence $A^2 \in \{D^2, 9D^2\}$. If $A^2 = D^2$, then $B = (A^2 - \Delta)/4 = D^2$, hence $(A, B) > 1$ or $A^2 = B = 1$; if $A^2 = 9D^2$, then $B = (A^2 - \Delta)/4 = 3D^2$ and hence $3 \mid (A, B)$. This leads to a contradiction.

Next we show (4).

Let $u'_0 = 0$, $u'_1 = 1$ and $u'_{j+1} = v_q u'_j - B^q u'_{j-1}$ for $j = 1, 2, 3, \cdots$. Note that $\alpha^q + \beta^q = v_q$ and $\alpha^q \beta^q = B^q$. Fix $k \in \mathbb{Z}^+$. If $\Delta = A^2 - 4B \neq 0$, then

$$\frac{u_{kq}}{u_q} = \frac{(\alpha^{kq} - \beta^{kq})/(\alpha - \beta)}{(\alpha^q - \beta^q)/(\alpha - \beta)} = \frac{(\alpha^q)^k - (\beta^q)^k}{\alpha^q - \beta^q} = u'_k;$$

if $\Delta = 0$, then $\alpha = \beta = A/2$, $u_q = q(A/2)^{q-1}$, $u_{kq} = kq(A/2)^{kq-1}$ and

$$u'_k = \sum_{0 \le r < k} (\alpha^q)^r (\beta^q)^{k-1-r} = k \left(\frac{A}{2}\right)^{q(k-1)} = \frac{u_{kq}}{u_q}.$$

So we always have $u_{kq}/u_q = u'_k$. By (8),

$$\frac{u_{kq}}{ku_q} \equiv r_k \pmod{u_q} \quad \text{where } r_k = u_{q+1}^{k-1} + \begin{cases} (k-1)Au_q/2 & \text{if } 2 \mid u_q, \\ 0 & \text{otherwise.} \end{cases}$$

Notice that $(r_k, u_q) = 1$ if $2 \nmid u_q$, and $(r_k, u_q/2) = 1$ if $2 \mid u_q$.

Suppose $m > n > 0$. We assert that

$$\prod_{0 \le k < n} \frac{u_{(m-k)q}}{u_{(n-k)q}} \equiv \binom{m}{n} u_{q+1}^{n(m-n)} \pmod{u_q}. \tag{10}$$

If $2 \nmid u_q$ or $4 \mid u_q$, then $(r_k, u_q) = 1$ for all $k = 1, 2, 3, \cdots$, hence

$$\begin{aligned} \prod_{0 \le k < n} \frac{u_{(m-k)q}}{u_{(n-k)q}} &= \prod_{0 \le k < n} \frac{m-k}{n-k} \times \prod_{0 \le k < n} \frac{u_{(m-k)q}/((m-k)u_q)}{u_{(n-k)q}/((n-k)u_q)} \\ &\equiv \binom{m}{n} \prod_{0 \le k < n} \frac{u_{q+1}^{m-k-1} + (m-k-1)Au_q/2}{u_{q+1}^{n-k-1} + (n-k-1)Au_q/2} \\ &\equiv \binom{m}{n} \prod_{0 \le k < n} \left(u_{q+1}^{m-n} + (m-n)A\frac{u_q}{2}\right) \equiv \binom{m}{n} \left(u_{q+1}^{n(m-n)} + n(m-n)A\frac{u_q}{2}\right) \\ &\equiv \binom{m}{n} u_{q+1}^{n(m-n)} + \frac{m(m-1)}{2}\binom{m-2}{n-1} Au_q \equiv \binom{m}{n} u_{q+1}^{n(m-n)} \pmod{u_q}. \end{aligned}$$

In the case $u_q \equiv 2 \pmod 4$, by the above method

$$\prod_{0 \le k < n} \frac{u_{(m-k)q}}{u_{(n-k)q}} \equiv \binom{m}{n} u_{q+1}^{n(m-n)} \pmod{\frac{u_q}{2}};$$

as $v_q = 2u_{q+1} - Au_q \equiv 0 \pmod 2$ and $B \equiv 1 \pmod 2$ (otherwise $A, u_1, u_2, u_3, \cdots$ are all odd), we also have

$$\prod_{0 \le k < n} \frac{u_{(m-k)q}}{u_{(n-k)q}} = \prod_{0 \le k < n} \frac{u'_{m-k}}{u'_{n-k}} \equiv \binom{m}{n} \equiv \binom{m}{n} u_{q+1}^{n(m-n)} \pmod 2$$

by Lemma 1. This proves (10).

Now we claim that

$$\begin{bmatrix} mq \\ nq \end{bmatrix} \equiv \binom{m}{n} u_{q+1}^{(m-n)nq} \pmod{w_q}. \tag{11}$$

This is obvious if $m \le n$ or $n = 0$. In the case $m > n > 0$, if $0 < j < nq$ and $q \nmid j$, then $(u_{nq-j}, w_q) = 1$ and

$$\frac{u_{mq-j}}{u_{nq-j}} = \frac{u_{(m-n)q+nq-j}}{u_{nq-j}} \equiv u_{q+1}^{m-n} \pmod{w_q}$$

by Lemma 3; thus

$$\begin{aligned}\begin{bmatrix} mq \\ nq \end{bmatrix} &= \prod_{0 \le j < nq} \frac{u_{mq-j}}{u_{nq-j}} = \prod_{0 \le k < n} \frac{u_{(m-k)q}}{u_{(n-k)q}} \times \prod_{\substack{0<j<nq \\ q \nmid j}} \frac{u_{mq-j}}{u_{nq-j}} \\ &\equiv \binom{m}{n} u_{q+1}^{n(m-n)} \times u_{q+1}^{(m-n)(nq-n)} = \binom{m}{n} u_{q+1}^{(m-n)nq} \pmod{w_q}.\end{aligned}$$

In view of (9) and (11),

$$\begin{aligned}\begin{bmatrix} mq+s \\ nq+t \end{bmatrix} &\equiv \binom{m}{n} u_{q+1}^{(m-n)nq} \times \begin{bmatrix} s \\ t \end{bmatrix} u_{q+1}^{t(m-n)+n(s-t)} \\ &\equiv \binom{m}{n} \begin{bmatrix} s \\ t \end{bmatrix} u_{q+1}^{(nq+t)(m-n)+n(s-t)} \pmod{w_q}.\end{aligned}$$

Finally we say something about (5). If $2 \mid q$, then

$$(nq+t)(m-n) + n(s-t) \equiv t(m-n) + n(s-t) \equiv mt - ns \pmod{2},$$

and $u_{q+1} \equiv -B^{q/2} \pmod{w_q}$ by Lemma 2. When q is odd and $l = m(n+t)+n(s+1)$ is even,

$$(nq+t)(m-n) + n(s-t) \equiv (n+t)(m-n) + n(s-t) \equiv l \equiv 0 \pmod{2}$$

and $u_{q+1}^2 \equiv B^q \pmod{w_q}$ by Lemma 2. Thus (5) follows from (4) if $2 \mid ql$. We are done.

Acknowledgement

The authors are indebted to the referee for his (or her) helpful suggestions.

References

1. L. E. Dickson, *History of the Theory of Numbers*, vol. I, Chelsea, New York, 1952, p. 396. MR **39:**6807a
2. R. D. Fray, *Congruence properties of ordinary and q-binomial coefficients*, Duke Math. J. **34** (1967), 467–480. MR **35:**4151
3. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in mathematics; 84), 2nd ed., Springer-Verlag, New York, 1990, pp. 191–192. MR **92e:**11001
4. W. A. Kimball and W. A. Webb, *Some congruences for generalized binomial coefficients*, Rocky Mountain J. Math. **25** (1995), 1079–1085. MR **96i:**11004
5. D. E. Knuth and H. S. Wilf, *The power of a prime that divides a generalized binomial coefficient*, J. Reine Angew. Math. **396** (1989), 212–219. MR **90d:**11029
6. A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33. MR **49:**8961
7. C. L. Stewart, *Primitive divisors of Lucas and Lehmer sequences, in:* Transcendence Theory: Advances and Applications (A. Baker and D.W. Masser, eds.), Academic Press, New York, 1977, pp. 79–92. MR **57:**16187
8. Zhi-Wei Sun, *Reduction of unknowns in Diophantine representations*, Scientia Sinica (Ser. A) **35** (3) (1992), 257–269. MR **93h:**11039

9. P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. **64** (1995), 869–888. MR **95f:**11022
10. B. Wilson, *Fibonacci triangles modulo p*, Fibonacci Quart. **36** (1998), 194–203. MR **99d:**11014

Department of Mathematics, Huaiyin Normal College, Huaiyin 223001, Jiangsu Province, People's Republic of China

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: zwsun@nju.edu.cn