ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 37, Number 3, 2007

CONGRUENCES FOR LUCAS u-NOMIAL COEFFICIENTS MODULO p^3

LING-LING SHI

ABSTRACT. In this paper we prove two congruences modulo p^2, p^3 (where $p > 3$ is prime) for generalized coefficients, *Lucas u-nomial coefficients* defined in terms of order recurrent sequences with initial values 0 and 1.

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

$$(1) \qquad u_0 = 0, \quad u_1 = 1, \quad \text{and} \quad u_{n+1} = Au_n - Bu_{n-1} \quad \text{for} \quad n \in \mathbf{N}.$$

(In the case $A = 1$ and $B = -1$, this yields the Fibonacci sequence $\{F_n\}_{n\geq 0}$.) Its companion sequence $\{v_n\}_{n\in\mathbf{N}}$ is given by

$$(2) \qquad v_0 = 2, \quad v_1 = A, \quad \text{and} \quad v_{n+1} = Av_n - Bv_{n-1} \quad \text{for} \quad n \in \mathbf{N}.$$

It is well known that

$$u_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } \Delta \neq 0, \\ n(A/2)^{n-1} & \text{if } \Delta = 0, \end{cases} \quad \text{and} \quad v_n = \alpha^n + \beta^n,$$

where

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

It follows that

$$2u_{m+n} = u_m v_n + u_n v_m, \quad v_{2n} = u_n v_n$$

and

$$v_{2n} = v_n^2 - 2B^n \quad \text{for} \quad n \in \mathbf{N}.$$

2000 AMS *Mathematics Subject Classification.* Primary 11B37, 11B65.
Received by the editors on June 7, 2004, and in revised form on Dec. 2, 2004.

For $x, y \in \mathbf{Z}$, let (x, y) denote the greatest common divisor of x and y. Lucas in [**1**] showed that if $(A, B) = 1$, then $(u_m, u_n) = |u_{(m,n)}|$ for $m, n \in \mathbf{N}$. It is known that $u_n \neq 0$ for all $n \in \mathbf{Z}^+$ except that $A^2 = B = 1$.

We set

$$[n] = \prod_{k=1}^{n} u_k, \quad [n]^F = \prod_{k=1}^{n} F_k, \quad [n]_j = \prod_{k=1}^{n} u_{kj} \quad \text{and} \quad [n]_j^F = \prod_{k=1}^{n} F_{kj}.$$

for $n \in \mathbf{N}$, and regard an empty product as value 1. For $n, k \in \mathbf{N}$ with $[n] \neq 0$, we define the *Lucas u-nomial coefficient* $\left[{n \atop k} \right]$ and *Fibonomial coefficient* $\left[{n \atop k} \right]^F$ as follows:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{cases} [n]/([k][n-k]) & \text{if } n \geq k, \\ 0 & \text{otherwise.} \end{cases}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}^F = \begin{cases} [n]^F/([k]^F[n-k]^F) & \text{if } n \geq k, \\ 0 & \text{otherwise.} \end{cases}$$

Or, more generally,

$$\begin{bmatrix} n \\ k \end{bmatrix}_j = \begin{cases} [n]_j/([k]_j[n-k]_j) & \text{if } n \geq k, \\ 0 & \text{otherwise.} \end{cases}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_j^F = \begin{cases} [n]_j^F/([k]_j^F[n-k]_j^F) & \text{if } n \geq k, \\ 0 & \text{otherwise,} \end{cases}$$

where $\{u_{ij}/u_j\}_{i \in \mathbf{N}}$ is also a Lucas sequence, i.e., $\{u_i(v_i, B^j)\}_{i \geq 0}$. In the case $A = 2$ and $B = 1$, $\left[{n \atop k} \right]$ coincides with the usual binomial coefficient $\binom{n}{k}$ because $u_n = n$. When $A = q + 1$ and $B = q$ where $q \in \mathbf{Z}$ and $|q| > 1$, $\left[{n \atop k} \right]$ is exactly the Gaussian q-nomial coefficient $\binom{n}{k}_q$ because $u_j = (q^j - 1)/(q - 1)$ for $j \in \mathbf{N}$. For generalized binomial coefficients formed from an arbitrary sequence of positive integers, see [**7**].

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

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

this property is usually called the *regular divisibility* of $\{u_n\}_{n\in\mathbf{N}}$. 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 $(A, B) = 1$, $q = d^*$, $n \in \mathbf{N}$ 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.

Here are two well-known properties concerning binomial coefficients [**1, 4**]:

(1) For any prime $p > 3$, we have

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}.$$

(2) (*Lucas's theorem*). For $a, b, s, t \in \mathbf{N}$ with $s, t < p$, we have

$$\binom{ap+s}{bp+t} \equiv \binom{a}{b}\binom{s}{t} \pmod{p}.$$

In 1995, Kimball and Webb [**3, 6**] proved the following congruences for generalized binomial coefficients:

$$\begin{aligned}
\begin{bmatrix} \tau a \\ \tau b \end{bmatrix}^F &\equiv \binom{ta}{tb} \pmod{p^2},\\
\begin{bmatrix} ar \\ br \end{bmatrix}^F &\equiv \varepsilon^{(a-b)br} \begin{bmatrix} a \\ b \end{bmatrix}^F \pmod{p^2},\\
\begin{bmatrix} ar \\ br \end{bmatrix} &\equiv \left(\frac{v_r}{2}\right)^{(a-b)br} \binom{a}{b} \pmod{p^2},
\end{aligned}$$

where τ is the period of the Fibonacci sequence modulo an odd prime p, r is the rank of apparition of p (that is, F_r is the first nonzero F_i divisible by p), and $t = \tau/r$ is an integer. In [**9**] it is shown that $t \in \{1, 2, 4\}$. The number ε is defined as follows: $\varepsilon = 1$ if $\tau = r$; $\varepsilon = -1$ if $\tau = 2r$; and $\varepsilon^2 \equiv -1 \pmod{p^2}$ if $\tau = 4r$, in this case $p \equiv 1 \pmod 4$.

They [**4**] also proved that for any prime $p > 3$ and any $a \geq b \geq 0$, if $r = p \pm 1$, then

$$\begin{bmatrix} ar \\ br \end{bmatrix}^F \equiv (\mp 1)^{(a-b)b} \begin{bmatrix} a \\ b \end{bmatrix}_r^F \pmod{p^3}. \tag{3}$$

In 1998, Wilson [**10**] proved that for any prime $p \neq 2, 5$, we have

$$\begin{bmatrix} ar \\ br \end{bmatrix}^F \equiv \begin{bmatrix} a \\ b \end{bmatrix}^F F_{r+1}^{(a-b)br} \pmod{p},$$

and

$$\begin{bmatrix} ar+s \\ br+t \end{bmatrix}^F \equiv \binom{a}{b} \begin{bmatrix} s \\ t \end{bmatrix}^F F_{r+1}^{(br+t)(a-b)+b(s-t)} \pmod{p}.$$

In 2001, Hu and Sun [**2**] proved the following result which extends Lucas's theorem as well as a result of Wilson:

Suppose that $(A, B) = 1$ and $A \neq \pm 1$ or $B \neq 1$. Then $u_k \neq 0$ for $k \in \mathbf{Z}^+$. Let $q \in \mathbf{Z}^+$, $a, b, s, t \in \mathbf{N}$ and $0 \leq s,\ t < q$. Then

$$\begin{bmatrix} aq+s \\ bq+t \end{bmatrix} \equiv \binom{a}{b} \begin{bmatrix} s \\ t \end{bmatrix} u_{q+1}^{(bq+t)(a-b)+b(s-t)} \pmod{w_q},$$

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

In this paper, we study two congruences modulo p^2, p^3 (where $p > 3$ is prime) for Lucas u-nomial coefficients. The main results are as follows:

Theorem 1. *Suppose that $(A, B) = 1$, and $A \neq \pm 1$ or $B \neq 1$. Let $p > 3$ be a prime not dividing B. If the rank r of apparition of p is $p+1$ or $p-1$ (and hence $r = p - (\frac{A^2-4B}{p})$), then for any $a, b \in \mathbf{N}$ we have*

$$\begin{bmatrix} ar \\ br \end{bmatrix} \equiv (-1)^{(a-b)b} B^{(a-b)b\binom{r}{2}} \begin{bmatrix} a \\ b \end{bmatrix}_r \pmod{p^3}. \tag{4}$$

Remark 1. In the case $A = -B = 1$, this yields the theorem of Kimball and Webb [**4**]. Here, from the fact that if $(A, B) = 1$, $p \nmid B\Delta$

and $u_{p-(\frac{\Delta}{p})} \equiv 0 \pmod p$, then $p \mid u_{(p-(\frac{\Delta}{p}))/2} \Leftrightarrow (\frac{B}{p}) = 1$. We can know $p \equiv 3 \pmod 4$ for $B = -1$ and $r = p \pm 1 = p - (\frac{\Delta}{p})$.

Theorem 2. *Suppose that $(A, B) = 1$ and $A \neq \pm 1$ or $B \neq 1$. Let $p > 3$ be a prime not dividing B. If r is the rank of apparition of p, then for any $a, b, s, t \in \mathbf{N}$ and $0 \leq s,\ t < r$, we have*

(5)

$$\begin{bmatrix} ar+s \\ br+t \end{bmatrix} \equiv \begin{cases} (-1)^{t-s-1} B^{-\binom{t-s}{2}} u_{(a-b)r}\, u_{t-s}^{-1} \\ \times\, u_{r+1}^{(a-b)(t-1)-b(t-s)} \begin{bmatrix} ar \\ br \end{bmatrix} \begin{bmatrix} t \\ s \end{bmatrix}^{-1} \pmod{p^2} & \text{if } s < t, \\ u_{r+1}^{at+bs-2bt} \dfrac{S_{a,s}}{S_{b,t} S_{a-b,s-t}} \begin{bmatrix} ar \\ br \end{bmatrix} \begin{bmatrix} s \\ t \end{bmatrix} \pmod{p^2} & \text{if } s \geq t, \end{cases}$$

where $S_{k,n} = 1 - (kBu_r)/u_{r+1} \sum_{j=1}^{n} (u_{j-1}/u_j)$.

If $p \nmid \Delta$, then $\left[\begin{smallmatrix} ar \\ br \end{smallmatrix}\right]$ in (5) can be replaced by $(v_r/2)^{(a-b)br} \binom{a}{b}$.

Remark 2. In the above two theorems, $p > 3$ can't be replaced by $p \geq 3$ because there exist counterexamples for $p = 3$.

Example 1. For $p = 3$ (in this case $r = 2$). If $A = 2$, $B = 1$, $a = 2$, $b = 1$, then

$$\begin{bmatrix} ar \\ br \end{bmatrix} = \binom{ar}{br} = \binom{4}{2} = 6, \quad \text{and} \quad (-1)^{(a-b)b} B^{(a-b)b\binom{r}{2}} \begin{bmatrix} a \\ b \end{bmatrix}_r = -2.$$

Obviously, $6 \not\equiv -2 \pmod{3^3}$.

Example 2. For $p = 3$ (in this case $r = 2$). If $A = 2$, $B = 1$, $a = 2$, $b = 1$, $s = 2$, $t = 1$, then

$$\begin{bmatrix} ar+s \\ br+t \end{bmatrix} = \binom{6}{3} = 20, \quad \text{and} \quad u_{r+1}^{at+bs-2bt} \frac{S_{a,s}}{S_{b,t} S_{a-b,s-t}} \begin{bmatrix} ar \\ br \end{bmatrix} \begin{bmatrix} s \\ t \end{bmatrix} = 36.$$

Obviously, $20 \not\equiv 36 \pmod{3^2}$.

2. Several lemmas and propositions.

Lemma 1 [**2**]. *Suppose that* $(A,B)=1$ *and* $A\neq\pm1$ *or* $B\neq 1$. *Then* $u_k\neq 0$ *for* $k\in\mathbf{Z}^+$.

Lemma 2 [**5**]. *Let* $p>3$ *be prime and* r *the rank of apparition of* p. *Then*

$$\sum_{k=1}^{r-1}\frac{v_k}{u_k}\equiv 0 \pmod p.$$

Moreover, if $r=p\pm1$, *then*

$$\sum_{k=1}^{r-1}\frac{v_k}{u_k}\equiv 0 \pmod{p^2}.$$

Corollary 1.

$$\frac{1}{2}\left(\frac{v_{mr}}{2}\right)^{r-2}\left(u_{mr}+\frac{v_r u_{mr}^2}{v_{mr}u_r}\right)\sum_{k=1}^{r-1}\frac{v_k}{u_k}\equiv 0 \pmod{p^3}.$$

Lemma 3. *Let* $p>3$ *be prime and* r *the rank of apparition of* p. *Then*

$$\sum_{k=1}^{r-1}\left(\frac{v_k}{u_k}\right)^2\equiv (r-1)\Delta-\sum_{k=1}^{r-1}\frac{2v_r}{u_k u_{r-k}} \pmod{p^2}.$$

Proof. Clearly,

$$\begin{aligned}(u_k v_{r-k})^2+(u_{r-k}v_k)^2+2u_k v_{r-k}u_{r-k}v_k &= (u_k v_{r-k}+u_{r-k}v_k)^2\\ &= (2u_r)^2\equiv 0 \pmod{p^2};\end{aligned}$$

therefore,

$$2\sum_{k=1}^{r-1}\left(\frac{v_k}{u_k}\right)^2=\sum_{k=1}^{r-1}\left(\left(\frac{v_k}{u_k}\right)^2+\left(\frac{v_{r-k}}{u_{r-k}}\right)^2\right)$$

$$= \sum_{k=1}^{r-1} \frac{(v_k u_{r-k})^2 + (v_{r-k} u_k)^2}{(u_k u_{r-k})^2}$$
$$\equiv \sum_{k=1}^{r-1} \frac{-2u_k v_{r-k} u_{r-k} v_k}{(u_k u_{r-k})^2}$$
$$\equiv -2 \sum_{k=1}^{r-1} \frac{v_k v_{r-k}}{u_k u_{r-k}} \pmod{p^2}.$$

That is,

$$\sum_{k=1}^{r-1} \left(\frac{v_k}{u_k}\right)^2 \equiv -\sum_{k=1}^{r-1} \frac{v_k v_{r-k}}{u_k u_{r-k}} \pmod{p^2}.$$

As $2v_{k+(r-k)} = v_k v_{r-k} + \Delta u_k u_{r-k}$, we have

$$\Delta + \frac{v_k v_{r-k}}{u_k u_{r-k}} = \frac{2v_r}{u_k u_{r-k}}.$$

So

$$-\sum_{k=1}^{r-1} \frac{v_k v_{r-k}}{u_k u_{r-k}} = \sum_{k=1}^{r-1} \left(\Delta - \frac{2v_r}{u_k u_{r-k}}\right) = (r-1)\Delta - \sum_{k=1}^{r-1} \frac{2v_r}{u_k u_{r-k}},$$

and hence

$$\sum_{k=1}^{r-1} \left(\frac{v_k}{u_k}\right)^2 \equiv (r-1)\Delta - \sum_{k=1}^{r-1} \frac{2v_r}{u_k u_{r-k}} \pmod{p^2}. \qquad \square$$

Lemma 4. *Let $p > 3$ be prime and r the rank of apparition of p. Then*

$$\frac{\prod_{k=1}^{r-1} u_{mr+k}}{\prod_{k=1}^{r-1} u_k} \equiv \left(\frac{v_{mr}}{2}\right)^{r-1} - (r-1)\,\frac{\Delta}{8}\,u_{mr}^2 \left(\frac{v_{mr}}{2}\right)^{r-3} \pmod{p^3}.$$

Proof. From the identity $2u_{a+b} = u_a v_b + u_b v_a$, we can obtain $2u_{mr+k} = u_{mr} v_k + u_k v_{mr}$. As $p \mid u_r$ and $u_r \mid u_{mr}$, we have $p \mid u_{mr}$, and hence

(6)

$$2^{r-1} \prod_{k=1}^{r-1} u_{mr+k} \equiv (v_{mr}^{r-1} + v_{mr}^{r-2} u_{mr} \Sigma_1 + v_{mr}^{r-3} u_{mr}^2 \Sigma_2) \prod_{k=1}^{r-1} u_k \pmod{p^3},$$

where

$$\Sigma_1 = \sum_{k=1}^{r-1} \frac{v_k}{u_k}, \qquad \Sigma_2 = \sum_{1 \le i < k \le r-1} \frac{v_i v_k}{u_i u_k}.$$

Dividing both sides of (6) by $2^{r-1} \prod_{k=1}^{r-1} u_k$, we get

$$\frac{\prod_{k=1}^{r-1} u_{mr+k}}{\prod_{k=1}^{r-1} u_k} \equiv \left(\frac{v_{mr}}{2}\right)^{r-1} + \frac{1}{2}\left(\frac{v_{mr}}{2}\right)^{r-2} u_{mr}\Sigma_1 + \frac{1}{4}\left(\frac{v_{mr}}{2}\right)^{r-3} u_{mr}^2 \Sigma_2 \pmod{p^3}. \tag{7}$$

Note that

$$\begin{aligned} \Sigma_1^2 &= \left(\sum_{k=1}^{r-1} \frac{v_k}{u_k}\right)^2 \\ &= \sum_{k=1}^{r-1} \left(\frac{v_k}{u_k}\right)^2 + 2 \sum_{1 \le i < k \le r-1} \frac{v_i v_k}{u_i u_k} \\ &= \sum_{k=1}^{r-1} \left(\frac{v_k}{u_k}\right)^2 + 2\Sigma_2, \end{aligned}$$

and thus

$$\Sigma_2 = \frac{1}{2}\left(\Sigma_1^2 - \sum_{k=1}^{r-1} \left(\frac{v_k}{u_k}\right)^2\right). \tag{8}$$

From Lemma 2 and (8), we have

$$u_{mr}^2 \Sigma_2 \equiv -\frac{1}{2}\, u_{mr}^2 \sum_{k=1}^{r-1} \left(\frac{v_k}{u_k}\right)^2 \pmod{p^4}. \tag{9}$$

From Lemma 2, Lemma 3 and (9), we have

$$u_{mr}^2 \Sigma_2 \equiv -\frac{\Delta}{2}\,(r-1) u_{mr}^2 + u_{mr}^2 \sum_{k=1}^{r-1} \frac{u_r}{u_k u_{r-k}} \pmod{p^4},$$

and hence

$$u_{mr}^2\Sigma_2 \equiv -\frac{\Delta}{2}(r-1)u_{mr}^2 + v_r\,\frac{u_{mr}^2}{u_r}\sum_{k=1}^{r-1}\frac{v_r}{u_k u_{r-k}} \pmod{p^4}.$$

Since $\sum_{k=1}^{r-1} u_r/(u_k u_{r-k}) = \Sigma_1$ and

$$2\Sigma_1 = \sum_{k=1}^{r-1}\left(\frac{v_k}{u_k}+\frac{v_{r-k}}{u_{r-k}}\right) = \sum_{k=1}^{r-1}\frac{v_k u_{r-k}+u_k v_{r-k}}{u_k u_{r-k}} = \sum_{k=1}^{r-1}\frac{2u_r}{u_k u_{r-k}},$$

we have

$$u_{mr}^2\Sigma_2 \equiv -\frac{\Delta}{2}(r-1)u_{mr}^2 + v_r\,\frac{u_{mr}^2}{u_r}\,\Sigma_1 \pmod{p^4},$$

and thus

$$\frac{\prod_{k=1}^{r-1}u_{mr+k}}{\prod_{k=1}^{r-1}u_k} \equiv \left(\frac{v_{mr}}{2}\right)^{r-1} - \frac{\Delta}{8}\,u_{mr}^2\left(\frac{v_{mr}}{2}\right)^{r-3}(r-1) + \frac{1}{2}\left(\frac{v_{mr}}{2}\right)^{r-2}\left(u_{mr}+\frac{v_r u_{mr}^2}{v_{mr}u_r}\right)\Sigma_1 \pmod{p^3}.$$

So it follows from Corollary 1 that

$$\frac{\prod_{k=1}^{r-1}u_{mr+k}}{\prod_{k=1}^{r-1}u_k} \equiv \left(\frac{v_{mr}}{2}\right)^{r-1} - (r-1)\,\frac{\Delta}{8}\,u_{mr}^2\left(\frac{v_{mr}}{2}\right)^{r-3} \pmod{p^3}.$$

This ends the proof. □

Lemma 5. *Let* $k \in \mathbf{Z}^+$, $2 \mid r$. *Then*

$$v_{kr} \equiv (-1)^k 2B^{kr/2} \pmod{p^2}.$$

Proof. As

$$2v_{kr} = v_{(k-1)r}v_r + \Delta u_{(k-1)r}u_r,$$

we have

$$v_{kr} \equiv \frac{v_{(k-1)r}v_r}{2} \pmod{p^2}.$$

From $p \mid u_r$, $p \nmid u_{r/2}$ and $u_r = u_{r/2}v_{r/2}$, it is easy to obtain $p \mid v_{r/2}$. Therefore,

$$v_r = v_{r/2}^2 - 2B^{r/2} \equiv -2B^{r/2} \pmod{p^2}.$$

Thus, the desired result follows by induction on k.

Lemma 6. *If* $r = p \pm 1$, $p \nmid B$ *and* $[n] \neq 0$ *for* $n \in \mathbf{N}$, *then*

$$\begin{bmatrix} (m+1)r-1 \\ r-1 \end{bmatrix} \equiv (-1)^m B^{m\binom{r}{2}} \pmod{p^3}.$$

Proof. We deal with the two cases separately.

Case 1. $r = p+1$. In this case, from Lemma 4 we clearly have,

$$\begin{aligned}\frac{\prod_{k=1}^{r-1} u_{mr+k}}{\prod_{k=1}^{r-1} u_k} &\equiv \left(\frac{v_{mr}}{2}\right)^p - \frac{\Delta}{8}\, u_{mr}^2 \left(\frac{v_{mr}}{2}\right)^{p-2} p \equiv \left(\frac{v_{mr}}{2}\right)^p \\ &\equiv ((-1)^m B^{(mr)/2} + p^2 q)^p \equiv (-1)^{mp} B^{(mrp)/2} \\ &\equiv (-1)^m B^{m\binom{r}{2}} \pmod{p^3}.\end{aligned}$$

Case 2. $r = p-1$. In this case, from Lemma 4 we have

$$\begin{aligned}\begin{bmatrix} (m+1)r-1 \\ r-1 \end{bmatrix} &= \frac{\prod_{k=1}^{r-1} u_{mr+k}}{\prod_{k=1}^{r-1} u_k} \\ &\equiv \left(\frac{v_{mr}}{2}\right)^{p-2} - \frac{\Delta}{8}\, u_{mr}^2 \left(\frac{v_{mr}}{2}\right)^{p-4} (p-2) \\ &\equiv \frac{1}{4}\left(\frac{v_{mr}}{2}\right)^{p-4} (v_{mr}^2 + \Delta u_{mr}^2) \pmod{p^3}.\end{aligned}$$

Since $v_{mr}^2 + \Delta u_{mr}^2 = 2v_{mr}^2 - 4B^{mr}$, we have

$$\frac{1}{4}\left(\frac{v_{mr}}{2}\right)^{p-4} (v_{mr}^2 + \Delta u_{mr}^2) = 2\left(\frac{v_{mr}}{2}\right)^{p-2} - B^{mr}\left(\frac{v_{mr}}{2}\right)^{p-4}.$$

It follows from Lemma 5 that

$$\frac{v_{mr}}{2} = (-1)^m B^{(mr)/2} + p^2 q, \quad \text{for some} \quad q \in \mathbf{Z}.$$

Thus,

$$\begin{aligned}\left(\frac{v_{mr}}{2}\right)^{p-k} &= ((-1)^m B^{(mr)/2} + p^2 q)^{p-k} \\ &\equiv (-1)^{m(p-k)} B^{(mr(p-k))/2} + (p-k)p^2 q(-B^{r/2})^{m(p-k+1)}.\end{aligned}$$

Note that, for $r = p-1$, $p \nmid B$, we have

$$B^{r/2} \equiv \left(\frac{B}{p}\right) \pmod{p}.$$

Therefore,

$$\left(\frac{v_{mr}}{2}\right)^{p-k} \equiv \begin{cases} (-1)^{m(p-k)} B^{(mr(p-k))/2} - kp^2 q \pmod{p^3} & \text{if } \left(\frac{B}{p}\right) = -1, \\ (-1)^{m(p-k)} B^{(mr(p-k))/2} & \\ -(-1)^{m(p-k-1)} kp^2 q \pmod{p^3} & \text{if } \left(\frac{B}{p}\right) = 1. \end{cases}$$

In particular, if k is even, then we always have

$$\left(\frac{v_{mr}}{2}\right)^{p-k} \equiv (-1)^{m(p-k)} B^{(mr(p-k))/2} - kp^2 q \pmod{p^3},$$

and hence

$$\begin{aligned} &2\left(\frac{v_{mr}}{2}\right)^{p-2} - B^{mr}\left(\frac{v_{mr}}{2}\right)^{p-4} \\ &\quad \equiv 2((-1)^{m(p-2)} B^{(mr(p-2))/2} - 2p^2 q) \\ &\qquad - B^{mr}((-1)^{m(p-4)} B^{(mr(p-4))/2} - 4p^2 q) \\ &\quad \equiv (-1)^{mp} 2B^{(mr(p-2))/2} - 4p^2 q - (-1)^{mp} B^{(mr(p-2))/2} + 4p^2 q B^{mr} \\ &\quad \equiv (-1)^{mp} B^{(mr(p-2))/2} + 4p^2 q(B^{mr} - 1) \\ &\quad \equiv (-1)^m B^{m\binom{r}{2}} \pmod{p^3}, \end{aligned}$$

where we use Fermat's little theorem in the last step. This ends the proof. □

Proposition 1. *Let $m, n \in \mathbf{N}$. If $r = p \pm 1$, then*

$$\prod_{k=nr+1}^{nr+r-1} u_{mr+k} \equiv (-1)^m B^{m\binom{r}{2}} \prod_{k=nr+1}^{nr+r-1} u_k \pmod{p^3}.$$

Proof. By Lemma 6, we have

$$\prod_{k=nr+1}^{nr+r-1} u_{mr+k} = \prod_{k=1}^{r-1} u_{(m+n)r+k} \equiv (-1)^{m+n} B^{(m+n)\binom{r}{2}} \prod_{k=1}^{r-1} u_k \pmod{p^3}$$

and

$$\prod_{k=nr+1}^{nr+r-1} u_k = \prod_{k=1}^{r-1} u_{nr+k} \equiv (-1)^n B^{n\binom{r}{2}} \prod_{k=1}^{r-1} u_k \pmod{p^3}.$$

So

$$\begin{aligned} \frac{\prod_{k=nr+1}^{nr+r-1} u_{mr+k}}{\prod_{k=nr+1}^{nr+r-1} u_k} &\equiv \frac{(-1)^{m+n} B^{(m+n)\binom{r}{2}} \prod_{k=1}^{r-1} u_k}{(-1)^n B^{n\binom{r}{2}} \prod_{k=1}^{r-1} u_k} \\ &\equiv (-1)^m B^{m\binom{r}{2}} \pmod{p^3}, \end{aligned}$$

i.e.,

$$\prod_{k=nr+1}^{nr+r-1} u_{mr+k} \equiv (-1)^m B^{m\binom{r}{2}} \prod_{k=nr+1}^{nr+r-1} u_k \pmod{p^3}.$$

Lemma 7. *Let $k, q \in \mathbf{Z}^+$. Then for any $j \in \mathbf{N}$ we have*

$$u_{kq+j} \equiv \sum_{i=0}^{m-1} \binom{k}{i} u_{q+1}^{k-i} (-Bu_q)^i \, u_{j-i} \pmod{u_q^m}$$

for $m = 1, 2$.

Proof. By Lemma 2 of Sun [**8**],

$$u_{kq+j} = \sum_{i=0}^{k} \binom{k}{i} (-Bu_q)^{k-i}\, u_q^i\, u_{j+i}.$$

Note that $-Bu_{q-1} = u_{q+1} - Au_q \in \mathbf{Z}$. Clearly, $u_{kq+j} \equiv u_{q+1}^k u_j \pmod{u_q}$. For $m = 2$,

$$\begin{aligned} u_{kq+j} &= \sum_{i=0}^{k} \binom{k}{i} (u_{q+1} - Au_q)^{k-i}\, u_q^i\, u_{j+i} \\ &\equiv (u_{q+1} - Au_q)^k\, u_j + k(u_{q+1} - Au_q)^{k-1}\, u_q\, u_{j+1} \\ &\equiv u_{q+1}^k\, u_j - kAu_{q+1}^{k-1}\, u_q\, u_j + ku_{q+1}^{k-1} u_q\, u_{j+1} \\ &\equiv u_{q+1}^k\, u_j + ku_{q+1}^{k-1}\, u_q(u_{j+1} - Au_j) \\ &\equiv u_{q+1}^k\, u_j - kBu_{q+1}^{k-1}\, u_q\, u_{j-1} \pmod{u_q^2}. \qquad \square \end{aligned}$$

Lemma 8. *Let* $k, n \in \mathbf{N}$*, and*

$$S_{k,n} = 1 - \frac{kBu_r}{u_{r+1}} \sum_{j=1}^{n} \frac{u_{j-1}}{u_j}.$$

Then

$$\prod_{j=1}^{n} (u_{r+1}\, u_j - kBu_r\, u_{j-1}) \equiv u_{r+1}^n S_{k,n} \prod_{j=1}^{n} u_j \pmod{p^2}.$$

Proof. It is easy to obtain by simple calculation. $\square$

3. Proofs of the theorems.

Proof of Theorem 1. From Lemma 1, we have $u_k \neq 0$ for $k \in \mathbf{Z}^+$. By Proposition 1, we have

$$\begin{bmatrix} ar \\ br \end{bmatrix} = \frac{u_{ar} u_{ar-1} \cdots u_{(a-b)r+1}}{u_{br} u_{br-1} \cdots u_1}$$

$$
\begin{aligned}
&= \frac{u_{ar}u_{(a-1)r}\cdots u_{(a-b+1)r}}{u_{br}u_{(b-1)r}\cdots u_r}\,\frac{\prod_{k=(a-1)r+1}^{(a-1)r+r-1}u_k\cdots\prod_{k=(a-b)r+1}^{(a-b)r+r-1}u_k}{\prod_{k=(b-1)r+1}^{(b-1)r+r-1}u_k\cdots\prod_{k=1}^{r-1}u_k}\\
&= \begin{bmatrix} a \\ b \end{bmatrix}_r \cdot \prod_{n=0}^{b-1}\prod_{k=nr+1}^{nr+r-1}\frac{u_{(a-b)r+k}}{u_k}\\
&\equiv \begin{bmatrix} a \\ b \end{bmatrix}_r \cdot \prod_{n=0}^{b-1}((-1)^{(a-b)}B^{(a-b)\binom{r}{2}})\\
&= (-1)^{(a-b)b}B^{(a-b)b\binom{r}{2}}\begin{bmatrix} a \\ b \end{bmatrix}_r \pmod{p^3}.
\end{aligned}
$$

This ends the proof. □

Proof of Theorem 2. From Lemma 1, we have $u_k \neq 0$ for all $k \in \mathbf{Z}^+$. If $a < b$, then $ar + s < (a+1)r \leq br + t$ and hence $\left[\begin{smallmatrix} ar+s \\ br+t \end{smallmatrix}\right] = 0 = \left[\begin{smallmatrix} ar \\ br \end{smallmatrix}\right]$. Below we only need to consider $a \geq b \geq 0$. Observe that

$$
\begin{aligned}
\begin{bmatrix} ar+s \\ br+t \end{bmatrix} &= \frac{\prod_{j=(a-b)r+1}^{ar}u_j}{\prod_{j=1}^{br}u_j}\cdot\frac{\prod_{j=1}^{s}u_{ar+j}}{\prod_{j=1}^{t}u_{br+j}}\\
&\quad\times\begin{cases}\prod_{j=1}^{t-s-1}u_{(a-b)r-j} & \text{if } s<t,\\ \prod_{j=1}^{s-t}u_{(a-b)r+j}^{-1} & \text{if } s\geq t.\end{cases}
\end{aligned}
$$

Case 1. $0 \leq s < t < r$. By Lemma 2, Lemma 7 and the fact $p \mid u_{(a-b)r}$, we get

$$
\begin{aligned}
\begin{bmatrix} ar+s \\ br+t \end{bmatrix} &\equiv \begin{bmatrix} ar \\ br \end{bmatrix}\cdot u_{(a-b)r}\cdot\frac{\prod_{j=1}^{s}u_{r+1}^{a}u_j}{\prod_{j=1}^{t}u_{r+1}^{b}u_j}\cdot\prod_{j=1}^{t-s-1}u_{r+1}^{a-b}(-B^{-j})u_j\\
&\equiv \begin{bmatrix} ar \\ br \end{bmatrix}\cdot u_{(a-b)r}\cdot u_{r+1}^{(a-b)(t-1)-b(t-s)}\,\frac{[s][t-s-1]}{[t]}\,(-1)^{t-s-1}B^{-\binom{t-s}{2}}\\
&\equiv (-1)^{t-s-1}B^{-\binom{t-s}{2}}u_{(a-b)r}u_{t-s}^{-1}\\
&\quad\times u_{r+1}^{(a-b)(t-1)-b(t-s)}\begin{bmatrix} ar \\ br \end{bmatrix}\begin{bmatrix} t \\ s \end{bmatrix}^{-1} \pmod{p^2}.
\end{aligned}
$$

Case 2. $0 \le t \le s < r$. By Lemma 2, Lemma 7, Lemma 8 and the fact $p \mid u_r$, we get

$$\begin{aligned}\begin{bmatrix} ar+s \\ br+t \end{bmatrix} &\equiv \begin{bmatrix} ar \\ br \end{bmatrix} \cdot \frac{\prod_{j=1}^{s} u_{r+1}^{a-1}(u_{r+1}u_j - aBu_r u_{j-1})}{\prod_{j=1}^{t} u_{r+1}^{b-1}(u_{r+1}u_j - bBu_r u_{j-1})} \\ &\quad \cdot \prod_{j=1}^{s-t} u_{r+1}^{b+1-a}(u_{r+1}u_j - (a-b)Bu_r u_{j-1})^{-1} \\ &\equiv \begin{bmatrix} ar \\ br \end{bmatrix} u_{r+1}^{at+bs-2bt} \cdot \frac{\prod_{j=1}^{s}(u_{r+1}u_j - aBu_r u_{j-1})}{\prod_{j=1}^{t}(u_{r+1}u_j - bBu_r u_{j-1})} \\ &\quad \cdot \prod_{j=1}^{s-t}(u_{r+1}u_j - (a-b)Bu_r u_{j-1})^{-1} \pmod{p^2}.\end{aligned}$$

So from Lemma 5, we have

$$\begin{aligned}\begin{bmatrix} ar+s \\ br+t \end{bmatrix} &\equiv \begin{bmatrix} ar \\ br \end{bmatrix} u_{r+1}^{at+bs-2bt} \cdot \frac{u_{r+1}^{s} S_{a,s}[s]}{u_{r+1}^{t} S_{b,t}[t][s-t]} \cdot u_{r+1}^{t-s} S_{a-b,s-t}^{-1} \\ &\equiv u_{r+1}^{at+bs-2bt} \, \frac{S_{a,s}}{S_{b,t} S_{a-b,s-t}} \begin{bmatrix} ar \\ br \end{bmatrix} \begin{bmatrix} s \\ t \end{bmatrix} \pmod{p^2}.\end{aligned}$$

Moreover, if $p \nmid \Delta$, then

$$\begin{bmatrix} ar \\ br \end{bmatrix} \equiv \left(\frac{v_r}{2}\right)^{(a-b)br} \binom{a}{b} \pmod{p^2}.$$

This concludes the proof. □

Acknowledgments. The author wishes to express her deepest thanks to her mentor, Professor Zhi-Wei Sun, for many helpful conversations, and to her friend, Li Wan, for his encouragement.

REFERENCES

1. L.E. Dickson, *History of the theory of numbers*, vol. I, Chelsea, New York, 1952, p. 396.

2. Hong Hu and Zhi-Wei Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478.

3. W.A. Kimball and W.A. Webb, *Congruence properties of Fibonacci numbers and Fibonacci coefficients*, in *Applications of Fibonacci numbers*, vol. 5, Kluwer, Dordrecht, 1993.

4. ———, *A congruence for Fibonacci coefficients modulo* p^3, Fibonacci Quart. **33** (1995), 290–297.

5. ———, *Some generalizations of Wolstenholme's theorem*, in *Applications of Fibonacci numbers*, vol. 8, Kluwer, Dordrecht, 1998, pp. 213–218.

6. ———, *Some congruences for generalized binomial coefficients*, Rocky Mountain J. Math. **25** (1995), 1079–1085.

7. 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.

8. Zhi-Wei Sun, *Reduction of unknowns in Diophantine representations*, Sci. Sinica **35** (1992), 257–269.

9. R.F. Torretoo and J.A. Fuchs, *Generalized binomial coefficients*, Fibonacci Quart. **2** (1964), 296–302.

10. B.Wilson, *Fibonacci triangles modulo p*, Fibonacci Quart. **36** (1998), 194–203.

College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua, Zhejiang 321004, P.R. China
E-mail address: linglingshi@zjnu.cn