Journal of Integer Sequences, Vol. 23 (2020),
Article 20.3.7

Another Lucasnomial Generalization of Wolstenholme's Congruence

Christian Ballot
Département de Mathématiques et Informatique
Université de Caen-Normandie
F14032 Caen Cedex
France
christian.ballot@unicaen.fr

Abstract

If $p \geq 5$ is a prime, then Wolstenholme's congruence stipulates that $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$. New generalizations of this congruence to Lucasnomials $\pmod{U_p^2 V_p / V_1}$ are given, where U and V are a pair of Lucas sequences.

1 Introduction

The binomial coefficient congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}, \tag{1}$$

valid for all primes $p \geq 5$, was established by Wolstenholme [21] in 1862.

Glaisher ([9, p. 21], [10, p. 33]) later gave the slightly more general congruence

$$\binom{(k+1)p-1}{p-1} \equiv 1 \pmod{p^3}, \tag{2}$$

for all nonnegative integers k and all primes $p \geq 5$.

An interest in finding an analogue, or a generalization of the Wolstenholme or the Glaisher congruences for Lucasnomials appears in various papers [2, 4, 12, 13, 14, 19].

If $A = (a_n)_{n\geq 0}$ is a sequence of integers, $a_n \neq 0$ for $n > 0$, then generalized binomial coefficients, $\binom{m}{n}_A$, with respect to A are defined for $m \geq n \geq 0$ to be

$$\binom{m}{n}_A = \frac{a_m a_{m-1} \ldots a_{m-n+1}}{a_n a_{n-1} \ldots a_1},$$

if $m \geq n \geq 1$, and 1 if $n = 0$.

Lucasnomials $\binom{m}{n}_U$ are generalized binomial coefficients defined with respect to a fundamental Lucas sequence U. They turn out always to be integers. Given two nonzero integers P and Q, the *fundamental Lucas sequence* $U = U(P, Q)$ is the second-order linear recurring sequence that satisfies the recursion

$$U_{n+2} = PU_{n+1} - QU_n, \tag{3}$$

for all integers n, and has initial conditions $U_0 = 0$ and $U_1 = 1$.

If $U_n \neq 0$ for all $n \geq 1$, then U is said to be *nondegenerate*. A necessary and sufficient condition for U to be nondegenerate is that $U_{12} \neq 0$. Lucas sequences U are *divisibility* sequences, i.e., they satisfy

$$m \mid n \implies U_m \mid U_n,$$

for all $n \geq m \geq 1$. If $\gcd(P, Q) = 1$, then $U(P, Q)$ is called *regular*. If U is regular, then it satisfies

$$\gcd(U_m, U_n) = |U_{\gcd(m,n)}|,$$

for all nonnegative m and n, not both zero. A sequence with this property is a *strong divisibility* sequence. A prime p is *regular* with respect to $U(P, Q)$ if $p \nmid \gcd(P, Q)$. An integer m is said to be *regular* if all its prime factors are regular. A *special* prime is one that divides $\gcd(P, Q)$. By extension an integer m is said to be *special* if all its prime factors are special. If $m \geq 2$ is an integer, then the *rank*, $\rho = \rho(m)$, of m is the least $t \geq 2$ for which $m \mid U_t$. It is guaranteed to exist if $\gcd(m, Q) = 1$. If $\gcd(m, Q) = 1$, then the rank ρ satisfies

$$m \mid U_n \iff \rho \mid n.$$

If $p \nmid Q$ is an odd prime, then $\rho(p)$ is a divisor of $p - (D \mid p)$, where $D = P^2 - 4Q$ and $(D \mid p)$ is the Legendre character of D with respect to p. The rank of p is *maximal* if $\rho(p) = p - (D \mid p)$. To every Lucas sequence $U(P, Q)$, there is an *associate*, or *companion* Lucas sequence V which satisfies the same recursion (3), but has initial values $V_0 = 2$, $V_1 = P$. If $D \neq 0$ and α and β denote the zeros of $x^2 - Px + Q$, then for all $n \geq 0$

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n. \tag{4}$$

We won't say much more about Lucas sequences, but refer interested readers to the original Lucas memoir [16], and to Chapter 4 of the book [20]. The reason why it is not unreasonable, with luck, to expect properties of ordinary binomial coefficients to extend to Lucasnomials

is that binomial coefficients are special Lucasnomials. Indeed, the binomial coefficients are the Lucasnomials attached to the fundamental Lucas sequence $U_n(2,1) = n$.

In [4], one finds two distinct generalizations of (2) for Lucasnomials. The first, which appeared in a weaker form in [19, Lemma 6], received a fully detailed proof and is stated below as a theorem. It is actually a concatenation of Theorems 3 and 7 in [4].

Theorem 1. *Let $U = U(P,Q)$ be a fundamental Lucas sequence with parameters P and Q. If a prime $p \geq 3$, $p \nmid Q$, has rank ρ in $U(P,Q)$, then the congruence*

$$\binom{(k+1)\rho - 1}{\rho - 1}_U \equiv (-1)^{k(\rho-1)} Q^{k\rho(\rho-1)/2} \pmod{p^\nu}, \tag{5}$$

holds for all integers $k \geq 0$ with

$$\nu = 2 + [\, p \geq 5 \,] \cdot [\, \rho \text{ is maximal} \,].$$

In the statement of the theorem we made use of the Iverson symbol $[-]$, where $[\mathcal{P}]$ is 1, if $\mathcal{P}$ is a true statement, and $[\mathcal{P}]$ is 0 otherwise. That is,

$$\nu = \begin{cases} 3, & \text{if } \rho \text{ is maximal and } p > 3; \\ 2, & \text{otherwise.} \end{cases}$$

In stating Theorem 1, one would expect the Lucas sequence U to be nondegenerate. However, with the convention that two zero-terms, one in the numerator, the other in the denominator of a Lucasnomial, cancel out as 1, the theorem holds even in the degenerate case [4].

The second generalization, [4, Thm. 9], went as follows:

Theorem 2. *Suppose $U(P,Q)$ is a nondegenerate regular fundamental Lucas sequence and $p \geq 3$ is a prime. Then*

$$\binom{(k+1)p - 1}{p - 1}_U \equiv Q^{kp(p-1)/2} \pmod{U_p^2},$$

for all $k \geq 0$.

When $|U_p| > 1$, p is the rank of U_p. Thus, as mentioned in [4], if $|U_p|$ is prime, then Theorem 2 follows from Theorem 1. Indeed, the hypotheses of Theorem 2 entail that if $|U_p|$ is prime, then $U_p \nmid Q$. For if $U_p \mid Q$, then, by (3), $U_p \equiv P^{p-1} \pmod{U_p}$, implying that $U_p \mid P$. This would contradict the regularity of U. For $U(1,-1)$, i.e., for the Fibonacci sequence, the congruence in Theorem 2 follows from the statement of a problem posed by Ohtsuka [18]. Mention was made in [4] that the published solution to the Ohtsuka problem [3] can be turned into a general proof of Theorem 2. This note provides a proof of Theorem 3, a more general theorem and a stronger congruence than Theorem 2, which, when U is the Fibonacci sequence, reduces to the initial problem [18] posed by Ohtsuka. We point out that the congruence holds irrespective of the regularity of $U(P,Q)$.

Theorem 3. *Suppose $U(P,Q)$ is a nondegenerate fundamental Lucas sequence and $p \geq 3$ is a prime. Then the congruence*

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{U_p^2 V_p/P},$$

holds for all $k \geq 0$, where $V(P,Q)$ is the companion Lucas sequence associated with U.

Remark 4. Theorem 3 does not hold with the modulus $U_p^2 V_p$. For instance, with $P = 5$, $Q = 1$ and $p = 5$, we find that $\binom{2p-1}{p-1}_U \equiv 153\,318\,506 \not\equiv 1 \pmod{U_p^2 V_p}$. Here, $U_5^2 V_5 = 766\,592\,525$, whereas $U_5^2 V_5/P = 153\,318\,505$.

Theorem 3 implies a stronger version of Theorem 2 where $U(P,Q)$ need not be regular, which is worth pointing out and stating.

Theorem 5. *Suppose $U(P,Q)$ is a nondegenerate fundamental Lucas sequence and $p \geq 3$ is a prime. Then for all $k \geq 0$*

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{U_p^2}.$$

Section 2 gives a proof of Theorem 3. We proceed roughly as follows. Put $M_p = U_p U_{2p}/P = U_p^2 V_p/P$. Let R_p be the largest regular integer factor of M_p, i.e., the largest factor of M_p prime to $\gcd(P,Q)$. Then $M_p = R_p S_p$, where S_p is the largest special factor of M_p. To prove the congruence of Theorem 3 modulo R_p, we will use a generalization of the non-published proof of Ohtsuka, who took the kind initiative to send it to the author in February 2015. Actually, for the prime $p = 3$, this approach immediately gives the congruence modulo M_3. (Two alternatives would have been either to use a generalization of the published solution [3] to Ohtsuka's problem [18], or to use Theorem 1. The first alternative is longer. The second can only yield the congruence modulo $\gcd(U_p^2, R_p)$.) To prove the congruence of Theorem 3 modulo S_p, given a special prime q it will suffice to show that both integers $\binom{(k+1)p-1}{p-1}_U$ and $Q^{kp(p-1)/2}$ have a q-adic valuation at least as high as that of M_p. We are able to prove the congruence modulo S_p in all cases because a full description [6] of the q-adic valuation of the terms of Lucas sequences exists. (Throughout the paper, if m is an integer, $\nu_q(m)$ denotes its q-adic valuation.) Actually, by Remark 19 of Section 4, proving the regular case only would have been sufficient to imply Theorem 3 in its full generality.

Section 3 gives some further results: In Proposition 16, we find a few instances of pairs $(U(P,Q), p)$ when Theorem 3 holds with respect to the modulus $U_p^3 V_p/P$.

Note that the congruence of Glaisher (2) gives

$$\binom{kp}{p} = \frac{kp}{p}\binom{kp-1}{p-1} \equiv \binom{k}{1} \pmod{p^3}.$$

It was generalized further [8] as follows: if $p \geq 5$ is prime and ℓ and k are nonnegative integers, then

$$\binom{kp}{\ell p} \equiv \binom{k}{\ell} \pmod{p^3}. \tag{6}$$

Kimball and Webb [15] gave an analogue of (6) for Fibonomials, i.e., Lucasnomials with respect to the Fibonacci sequence $U(1,-1)$, but modulo p^2. However, a Lucasnomial generalization of (6) along the line of Theorem 1 modulo p^3 exists [4, Thm. 13]. We give another, in line with Theorem 3, in Theorem 17.

Section 3 contains yet another proof of Theorem 3 for the case $p = 3$. This proof generalizes the proof given in the published solution [3] of Ohtsuka's problem [18].

The referee made some numerical experiments that suggested that a polynomial version of Theorem 3 might hold in the ring $\mathbb{Z}[P,Q]$ and that this polynomial version might also hold for $p = 2$ whenever 4 divides k. We added a new section to the paper to address the referee's questions. Section 4 contains Theorems 18 and 20 which prove the referee's observations to be exact.

2 Proof of Theorem 3

We begin with a generalized Cassini identity. This identity is proved [11] in a long and indirect manner using matrices and, probably, in other places as well. We give a very short and direct proof which uses the formulas (4) in the next lemma.

Lemma 6. *Suppose $U(P,Q)$ is a fundamental Lucas sequence with nonzero discriminant $D = P^2 - 4Q$. Then, for all $r \geq 0$, we have the identity*

$$U_a U_b - U_c U_d = Q^r (U_{a-r} U_{b-r} - U_{c-r} U_{d-r}),$$

provided $a + b = c + d$.

Proof. The quantity $U_t U_{n-t} - Q^r U_{t-r} U_{n-t-r}$ is independent of t. Indeed, if α and β are the distinct zeros of $x^2 - Px + Q$, then using $Q = \alpha\beta$ we obtain

$$\begin{aligned} D(U_t U_{n-t} - Q^r U_{t-r} U_{n-t-r}) &= (\alpha^t - \beta^t)(\alpha^{n-t} - \beta^{n-t}) - Q^r (\alpha^{t-r} - \beta^{t-r})(\alpha^{n-t-r} - \beta^{n-t-r}) \\ &= (\alpha^n + \beta^n - \alpha^t \beta^{n-t} - \beta^t \alpha^{n-t}) - Q^r (\alpha^{n-2r} + \beta^{n-2r}) + Q^r (\alpha^{t-r} \beta^{n-t-r} + \beta^{t-r} \alpha^{n-t-r}) \\ &= V_n - Q^r V_{n-2r}. \end{aligned}$$

Therefore, for all integers t and s, we see that

$$U_t U_{n-t} - Q^r U_{t-r} U_{n-t-r} = U_s U_{n-s} - Q^r U_{s-r} U_{n-s-r},$$

which yields the identity on putting $a = t$, $b = n - t$, $c = s$ and $d = n - s$. □

Lemma 7. *For all odd primes p and all integers $k \geq 1$, we have*

$$\binom{(k+1)p-1}{p-1}_U = \prod_{i=1}^{(p-1)/2} \left(\frac{U_{kp} U_{(k+1)p}}{U_i U_{p-i}} + Q^{kp} \right).$$

Proof. By Lemma 6, we see that

$$U_{(k+1)p-i}U_{kp+i} - U_{(k+1)p}U_{kp} = Q^{kp}(U_{p-i}U_i - U_pU_0).$$

Thus,

$$U_{(k+1)p-i}U_{kp+i} = U_{(k+1)p}U_{kp} + Q^{kp}U_{p-i}U_i.$$

Therefore,

$$\begin{aligned}\binom{(k+1)p-1}{p-1}_U &= \prod_{i=1}^{p-1}\frac{U_{kp+i}}{U_i} = \prod_{i=1}^{(p-1)/2}\frac{U_{(k+1)p-i}U_{kp+i}}{U_{p-i}U_i}\\ &= \prod_{i=1}^{(p-1)/2}\frac{U_{(k+1)p}U_{kp} + Q^{kp}U_{p-i}U_i}{U_{p-i}U_i}\\ &= \prod_{i=1}^{(p-1)/2}\left(\frac{U_{kp}U_{(k+1)p}}{U_iU_{p-i}} + Q^{kp}\right).\end{aligned}$$

□

Lemma 8. *Theorem 3 holds for $p = 3$.*

Proof. By Lemma 7, we obtain

$$\binom{(k+1)p-1}{p-1}_U = U_{kp}U_{(k+1)p}/P + Q^{kp} \equiv Q^{kp} = Q^{kp(p-1)/2} \pmod{M_p},$$

for $p = 3$ since $U_2 = P$ and U_pU_{2p} divides $U_{kp}U_{(k+1)p}$, where $M_p = U_pU_{2p}/P$. □

Lemma 9. *Suppose $q \nmid Q$ is a prime. Then, for all $n \geq 0$, $q \nmid \gcd(U_{n+1}, U_n)$.*

Proof. If not, there must exist a minimal integer $m \geq 1$ such that q divides U_m and U_{m+1}. Since $q \nmid \gcd(U_1, U_2)$, it must be that $m \geq 2$. But as $QU_{m-1} = PU_m - U_{m+1}$ and $q \nmid Q$, we see that $q \mid U_{m-1}$. Thus, $q \mid \gcd(U_{m-1}, U_m)$, which contradicts the minimality of m. □

Lemma 10. *Let q be a regular prime with respect to $U(P, Q)$. Then, for all $m \geq n > 0$, $\gcd(U_m, U_n)$ and $U_{\gcd(m,n)}$ share the same q-adic valuation.*

Proof. If $q \mid Q$, then $q \nmid U_n$ for any $n > 0$. Thus, the result holds in this case. Suppose $q \nmid Q$. Certainly, because U is a divisibility sequence, the q-adic valuation of $U_{\gcd(m,n)}$ is less than or equal to the q-adic valuation of $\gcd(U_m, U_n)$. Assume $q^\ell \mid \gcd(U_m, U_n)$. Then by the Lucas identity

$$U_m = U_{n+1}U_{m-n} - QU_nU_{m-n-1},$$

we see that $q^\ell \mid U_{n+1}U_{m-n}$. Since $q \nmid Q$ we know by Lemma 9 that q does not divide U_{n+1}. Thus, $q^\ell \mid U_{m-n}$. Therefore, $q^\ell \mid U_r$, where r is the first remainder in the Euclidean division of m by n. Reiterating the reasoning with n and r in place of m and n and, further, with any two successive remainders in the Euclidean division algorithm of m by n we find that q^ℓ divides $U_{\gcd(m,n)}$. □

Theorem 11. *The congruence of Theorem 3 holds modulo R_p, where R_p is the regular part of $M_p = U_pU_{2p}/P$.*

Proof. Both $U_{kp}U_{(k+1)p}$ and U_iU_{p-i} are divisible by $U_2 = P$ so that

$$\frac{U_{kp}U_{(k+1)p}}{U_iU_{p-i}} = \frac{U_{kp}U_{(k+1)p}/P}{U_iU_{p-i}/P}.$$

By Lemma 7, the theorem will hold if we show that for all i, $1 \le i \le (p-1)/2$, U_iU_{p-i}/P and R_p are coprime integers. Let q be a prime factor of R_p. Since i and $p-i$ are coprime, Lemma 10 tells us that $q \nmid \gcd(U_i, U_{p-i})$. Thus, with the notation $m \sim_q n$ meaning that $\nu_q(m) = \nu_q(n)$, we obtain

$$\begin{aligned}\gcd(U_iU_{p-i}, U_pU_{2p}) &\sim_q \gcd(U_i, U_pU_{2p}) \cdot \gcd(U_{p-i}, U_pU_{2p}) \\ &\sim_q \gcd(U_i, U_{2p}) \cdot \gcd(U_{p-i}, U_{2p}) \\ &\sim_q U_1U_2 = P\end{aligned}$$

Therefore, $\gcd(U_iU_{p-i}/P, M_p) \sim_q 1$. □

We now consider the congruence of Theorem 3 modulo special primes. Hence, throughout the remainder of this section q designates a special prime of $U(P,Q)$ with $P = q^aP'$ and $Q = q^bQ'$, $a \ge 1$, $b \ge 1$ and $q \nmid P'Q'$.

The q-adic valuation of the terms U_n, $(n \ge 1)$, is simplest in the case $b > 2a$. In this case, we have [6, Thm. 1.2] for all $n \ge 1$

$$\nu_q(U_n) = (n-1)a. \tag{7}$$

Lemma 12. *Suppose $U(P,Q)$ is a fundamental Lucas sequence and $p \ge 5$ is a prime. If q a special prime with $b > 2a$, then for all $k \ge 0$*

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{q^{\nu_q(M_p)}},$$

where $M_p = U_pU_{2p}/P$.

Proof. By (7), $\nu_q(M_p) = (p-1)a + (2p-1)a - a = 3(p-1)a$. Thus, to prove the lemma it suffices to see that both $\binom{(k+1)p-1}{p-1}_U$ and $Q^{kp(p-1)/2}$ have a q-adic valuation of at least $3(p-1)a$. Indeed, we have for all $k \ge 1$ and $p \ge 5$

$$\nu_q(Q^{kp(p-1)/2}) = bkp(p-1)/2 > ap(p-1) > 3(p-1)a. \tag{8}$$

Also as $\binom{(k+1)p-1}{p-1}_U = \prod_{i=1}^{p-1} \frac{U_{kp+i}}{U_i}$, we find using (7) that

$$\begin{aligned}\nu_q\left(\binom{(k+1)p-1}{p-1}_U\right) &= \sum_{i=1}^{p-1} \big((kp+i-1)a - (i-1)a\big) \\ &= \sum_{i=1}^{p-1} kpa = k(p-1)pa > 3(p-1)a.\end{aligned}$$

□

We now address the case $b = 2a$.

Lemma 13. *Suppose $U(P,Q)$ is a fundamental Lucas sequence and $p \geq 5$ is a prime. If q is a special prime with $b = 2a$, then for all $k \geq 0$*

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{q^{\nu_q(M_p)}},$$

where $M_p = U_p U_{2p}/P$.

Proof. If $b = 2a$, then, as seen in the proof of [6, Thm. 2.2], we have for all $n \geq 0$, $U_n = q^{(n-1)a} U'_n$, where U' is the Lucas sequence $U(P', Q')$. Thus,

$$\nu_q(M_p) = 3(p-1)a + \nu_q(M'_p),$$

where $M'_p = U'_p U'_{2p}/P'$. Since q is regular with respect to U', we find by Theorem 11 that

$$\binom{(k+1)p-1}{p-1}_{U'} \equiv (Q')^{kp(p-1)/2} \pmod{q^{\nu_q(M'_p)}}. \tag{9}$$

Since $U_n = q^{(n-1)a} U'_n$, we see that

$$\binom{(k+1)p-1}{p-1}_U = q^{kp(p-1)a} \binom{(k+1)p-1}{p-1}_{U'}.$$

But we also find that

$$Q^{kp(p-1)/2} = q^{kp(p-1)a} \cdot (Q')^{kp(p-1)/2}.$$

Thus multiplying the congruence (9) through by $q^{kp(p-1)a}$ we obtain

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{q^{\nu_q(M'_p)+kp(p-1)a}}.$$

Since $kp(p-1)a > 3(p-1)a$, we may degrade the modulus in the previous congruence and prove our lemma. □

If $b < 2a$, then by [6, Thm. 1.2]

$$\nu_q(U_{2n+1}) = bn, \tag{10}$$

while

$$\nu_q(U_{2n}) = bn + (a-b) + \nu_q(n) + c, \tag{11}$$

where c is a nonzero constant only if $q = 2$ or 3, $2a = b+1$ and $q \mid n$.

Lemma 14. *Suppose $U(P,Q)$ is a fundamental Lucas sequence and $p \geq 5$ is a prime. If q a special prime with $b < 2a$, then for all $k \geq 0$*

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{q^{\nu_q(M_p)}},$$

where $M_p = U_p U_{2p}/P$.

Proof. By equations (10) and (11), we calculate that

$$\nu_q(M_p) = 3b(p-1)/2 + \nu_q(p).$$

Indeed, by (11), for c to be nonzero, we need q to divide p, i.e., $q = p$. As $p \geq 5$, q is not equal to 2 or 3. Thus, $c = 0$.

Again we verify below that $\nu_q(Q^{kp(p-1)/2})$ exceeds $\nu_q(M_p)$ for all $k \geq 1$. For

$$\nu_q(Q^{kp(p-1)/2}) = kbp(p-1)/2 \geq 5b(p-1)/2 > 3b(p-1)/2 + \nu_q(p).$$

Now, assuming k is **even**, we write

$$\binom{(k+1)p-1}{p-1}_U = \prod_{i=1}^{p-1} \frac{U_{kp+i}}{U_i} = \prod_{i=1}^{(p-1)/2} \frac{U_{kp+2i}}{U_{2i}} \cdot \frac{U_{kp+2i-1}}{U_{2i-1}}.$$

In evaluating the q-adic valuation of $\binom{(k+1)p-1}{p-1}_U$, we make two observations. First, there are exactly $(p-1)/2$ even-indexed terms in both the numerator and the denominator of the above product. So the contribution of the quantities $(a-b)$ from equation (11) cancel out. The terms involving a nonzero quantity c require q to divide their index. We claim there are at least as many such indices among the '$kp+2i$' as among the '$2i$' so their total contribution to the q-adic valuation of $\binom{(k+1)p-1}{p-1}_U$ is nonnegative. If $q = 2$ this is clearly true. If $q = 3$, then 3 divides an integer in the interval $[1,(p-1)/2]$ exactly $\lfloor (p-1)/6 \rfloor$ times. It divides an integer in $[1+\frac{kp}{2}, \frac{p-1}{2}+\frac{kp}{2}]$ exactly $\lfloor (kp+p-1)/6 \rfloor - \lfloor (kp)/6 \rfloor$ times. But as for any two real numbers x and y, $\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$, we see that

$$\left\lfloor \frac{kp+p-1}{6} \right\rfloor \geq \left\lfloor \frac{p-1}{6} \right\rfloor + \left\lfloor \frac{kp}{6} \right\rfloor.$$

The total contribution of the quantities $\nu_q(n)$ which appear in (11) for even-indexed terms is given by

$$\nu_q\left(\prod_{i=1}^{(p-1)/2} \frac{kp/2+i}{i} \right) = \nu_q\left(\binom{kp/2+(p-1)/2}{(p-1)/2} \right) \geq 0,$$

since binomial coefficients are integers.

Thus, using again equations (10) and (11), we deduce that the q-adic valuation of $\binom{(k+1)p-1}{p-1}_U$ is at least

$$b\sum_{i=1}^{(p-1)/2}\big((kp/2+i)-i\big)+b\sum_{i=1}^{(p-1)/2}\big((kp/2+i-1)-(i-1)\big)=kbp(p-1)/2>\nu_q(M_p),$$

proving our claim. The case k **odd** can be treated similarly obtaining again the lower bound $kbp(p-1)/2$ for $\nu_q\big(\binom{(k+1)p-1}{p-1}_U\big)$. □

Thus gathering together Lemmas 12, 13 and 14, we have shown the following theorem.

Theorem 15. *Let $U=U(P,Q)$ be a nondegenerate fundamental Lucas sequence, $p\geq 5$ a prime, $k\geq 0$ an integer. Then*

$$\binom{(k+1)p-1}{p-1}_U\equiv Q^{kp(p-1)/2}\pmod{S_p},$$

where S_p is the largest special factor of $M_p=U_pU_{2p}/P$.

Since $M_p=R_pS_p$ and $\gcd(R_p,S_p)=1$, putting together Lemma 8 for the case $p=3$ and Theorems 11 and 15, we have a proof of Theorem 3.

3 Further complementary results

By Theorem 1, the condition '$|U_p|$ is prime and has maximal rank in U' is a sufficient condition for the congruence in Theorem 2 to hold modulo U_p^3. The next proposition describes all the cases when this rare condition is met. We recall first that a regular U is called *n-defective* if all primes of rank n divide D. We know that if $n>30$ and U is regular, then U is never n-defective [7]. Moreover, all cases of defectiveness were described in several tables [1, 7] using the parameters P and D. A single table [5, p. 33] describes all cases of defectiveness using the parameters P and Q.

Proposition 16. *Suppose $p\geq 5$ is prime and $|U_p|$ is a prime of maximal rank in U, where $U=U(P,Q)$, $P>0$, is a fundamental Lucas sequence other than $I=U(2,1)$. Then, either*

$$p=5\quad\text{and}\quad(P,Q)\in\{(1,-1),(1,4),(2,11)\},$$

or

$$p=7\quad\text{and}\quad(P,Q)=(1,2).$$

Thus, in these four cases, we find that

$$\binom{(k+1)p-1}{p-1}_U\equiv Q^{\frac{kp(p-1)}{2}}\pmod{U_p^3V_p/P},\tag{12}$$

for all $k\geq 0$.

Proof. Note that the hypotheses imply that $U(P,Q)$ is regular. For if a prime q divides $\gcd(P,Q)$, then, by [6, Thm. 1.1], U_p is at least divisible by $q^{(p-1)/2}$. As $p \geq 5$, this would contradict the primality of $|U_p|$. Because $|U_p|$ divides U_n at $n = p$ the rank of $|U_p|$ must divide p and thus be equal to p. If this rank is maximal, then $\rho(|U_p|) = p = |U_p| \pm 1$, or $|U_p|$. As $p \geq 5$, there are no two primes $|U_p|$ and p one apart from each other. Hence, $U_p = \pm p$. Not surprisingly this Diophantine equation has few solutions since U_n grows exponentially. But the condition $U_p = \pm p$ implies that $p \mid D$ and that U is p-defective. Therefore, $p \leq 30$ and we need only check those U in [5, Table A, p. 33] that are p-defective with $5 \leq p \leq 29$. Actually, there are only seven U that are 5-defective, two that are 7-defective and one which is 13-defective.

Suppose $p = 5$. The seven sequences correspond to $(P,Q) = (1,-1),\ (1,2),\ (1,3),\ (1,4),\ (2,11),\ (12,55)$ and $(12,377)$. The discriminant $D = P^2 - 4Q$ is divisible by 5 only for $(P,Q) = (1,-1),\ (1,4)$ and $(2,11)$. Since $U_5 = P^4 - 3P^2Q + Q^2$, it is easy to check that U_5 is ± 5 in these three cases. If $p = 7$, then $U(1,2)$ and $U(1,5)$ are 7-defective and their respective seventh terms are 7 and 1. The only 13-defective sequence is $U(1,2)$ with $D = -7$ not divisible by 13. Since $p = U_p$, $p \nmid Q$. By the identity $V_p^2 - DU_p^2 = 4Q^p$, we see that $\gcd(U_p, V_p) = 1$. Thus, the congruence (12) holds. □

Thus, for instance, if $U = U(1,2)$, $p = 7$ and $k = 1$, then $U_p = 7$, $V_p = -13$ and

$$\binom{2p-1}{p-1}_U - Q^{\frac{p(p-1)}{2}} = -9 \cdot 11 \cdot 17 \cdot 23 - 2^{21} = -7^3 \cdot 13 \cdot 499 \equiv 0 \pmod{U_p^3 V_p}.$$

However, again, the congruence modulo U_p^3 holds as a consequence of Theorem 1.

Note that Theorem 3 yields for all $k \geq 1$

$$\binom{kp}{p}_U = \binom{kp-1}{p-1}_U \cdot \frac{U_{kp}}{U_p} \equiv Q^{(k-1)p(p-1)/2} \binom{k}{1}_{U'} \pmod{U_p^2 V_p/P},$$

where $U'_n = U_{np}$. This can be generalized to all Lucasnomials of the type $\binom{kp}{\ell p}_U$.

Theorem 17. *Suppose $U = U(P,Q)$ is a fundamental Lucas sequence, $p \geq 3$ is a prime and $k \geq \ell \geq 0$ are integers. Then*

$$\binom{kp}{\ell p}_U \equiv Q^{(k-\ell)\ell\binom{p}{2}} \binom{k}{\ell}_{U'} \pmod{U_p^\nu V_p/P}, \tag{13}$$

where $U'_n = U_{pn}$ and $\nu = 2 + [\,p \geq 5\,] \cdot [\,U_p = \pm p\,]$.

Proof. It suffices to reproduce the proof of [4, Thm. 13] replacing ρ by p and the modulus p^3 by $U_p^\nu V_p/P$. The key point in the proof of [4, Thm. 13] was [4, Rmk. 4], which has an equivalent here, namely

$$\binom{(k+1)p-1}{p-1}_U \equiv \binom{2p-1}{p-1}_U^k \pmod{U_p^\nu V_p/P},$$

by Theorem 3 and Proposition 16. □

For the sake of curiosity we give another proof of Theorem 3 for the case $p = 3$, which generalizes the proof published for $p = 3$ in the Fibonacci case [3, p. 191].
Another proof of Theorem 3 for $p = 3$, i.e., of Lemma 8. Put

$$M := \frac{U_3^2 V_3}{P} = U_3 \cdot \frac{U_6}{P} = (P^2 - Q)(P^4 - 4P^2Q + 3Q^2) = P^6 - 5QP^4 + 7P^2Q^2 - 3Q^3.$$

One may observe that $a_k := \binom{3(k+1)-1}{3-1}_U = U_{3k+2}U_{3k+1}/P$ is a recurrent sequence. It is of the form $(A\alpha^{3k} + B\beta^{3k}) \cdot (C\alpha^{3k} + D\beta^{3k})$ for some constants A, B, C and D, where α and β are the zeros of $x^2 - Px + Q$. Thus, (a_k) is annihilated by the cubic polynomial

$$C(x) = (x - \alpha^6)(x - \beta^6)(x - Q^3) = x^3 - (Q^3 + V_6)x^2 + (Q^3V_6 + Q^6)x - Q^9.$$

For $k = -1, 0$ and 1, one can check that $a_k \equiv Q^{3k} \pmod{M}$. For instance,

$$a_1 = U_4U_5/P = (P^2 - 2Q)(P^4 - 3P^2Q + Q^2) = M + Q^3 \equiv Q^3 \pmod{M}.$$

Thus, that $a_k \equiv Q^{3k} \pmod{M}$, for all $k \geq 0$, easily follows by induction on noting that

$$C(x) = (x^3 - Q^9) - (Q^3 + V_6)(x^2 - Q^3x). \quad \square$$

4 A polynomial version of Theorem 3

The referee said he made some quick numerical experiments which indicated the congruence of Theorem 3 may hold in the polynomial ring $\mathbb{Z}[P, Q]$ and asked whether, if true, this statement is implied by Theorem 3. The two statements would then be clearly equivalent. We point out that the foregoing second proof of Theorem 3, for the case $p = 3$, at the end of Section 3, proves the $\mathbb{Z}[P, Q]$-statement is true when $p = 3$. We had played with a similar proof for the case $p = 5$, but writing a proof along these lines for general p seemed cumbersome. However, we are able to answer the referee's question in the positive in the next theorem. Note that the nondegeneracy hypothesis is no longer needed.

Theorem 18. *Let $p \geq 3$ be a prime number, $k \geq 0$ an integer and $\{U, V\}$ a pair of Lucas sequences with parameters P and Q. Then the congruence*

$$\binom{(k+1)p - 1}{p - 1}_U \equiv Q^{kp(p-1)/2} \pmod{U_p^2 V_p/P},$$

holds in the ring $\mathbb{Z}[P, Q]$.

Proof. As noted by Lucas [17, p. 312-13], U_n and V_n are homogeneous polynomials in $\mathbb{Z}[P, Q]$ of respective degrees $n - 1$ and n if one views the variable Q as being of degree 2. Moreover, as easily checked by induction on n using the recursion (3) each $U_n(P, Q)$, $n \geq 2$, is, as a polynomial in P, monic of leading term P^{n-1}, and each $V_n(P, Q)$, $n \geq 1$, is also monic

in P with leading term P^n. Thus the modulus $M(P,Q) = M_Q(P) := U_p^2 V_p/P$ is a monic polynomial in P in $\mathbb{Z}[Q][P]$. All Lucasnomials are also polynomials in $\mathbb{Z}[P,Q]$. This is often shown by induction using the identity:

$$\binom{m}{n}_U = U_{n+1}\binom{m-1}{n}_U - QU_{m-n-1}\binom{m-1}{n-1}_U.$$

Thus, we find that $f(P,Q) := \binom{(k+1)p-1}{p-1}_U - Q^{kp(p-1)/2}$ is a polynomial in $\mathbb{Z}[P,Q]$. Let us put $f(P,Q) = f_Q(P) \in \mathbb{Z}[Q][P]$. Then the euclidean division of $f_Q(P)$ by $M_Q(P)$ yields two polynomials $q_Q(P)$ and $r_Q(P)$ in $\mathbb{Z}[Q][P]$ satisfying

$$f_Q(P) = q_Q(P) \cdot M_Q(P) + r_Q(P), \tag{14}$$

with the degree in P of $r_Q(P)$ less than the degree of $M_Q(P)$. Indeed, $M_Q(P)$ is a monic polynomial in P so we know $q_Q(P)$ has polynomial coefficients in $\mathbb{Z}[Q]$. Therefore, $r_Q(P)$ is also in $\mathbb{Z}[Q][P]$. Let us fix Q to some nonzero value y in $\mathbb{Z}$. We may choose an integer value x for P large enough so that both $U_{12}(x,y) \neq 0$ and $|M_y(x)| > |r_y(x)|$. Thus, $U(x,y)$ is a nondegenerate fundamental Lucas sequence. Therefore, by Theorem 3, the integer $M_y(x)$ divides the integer $f_y(x)$. It follows from (14) that $M_y(x)$ divides $r_y(x)$. Thus, $r_y(x) = 0$ as an integer. Since there are arbitrarily many such integer values x for P, i.e., more than the degree of $r_y(P)$, we deduce that $r_y(P) = 0$ as a polynomial. Thus, the polynomial coefficients in $\mathbb{Z}[Q]$ of $r_Q(P)$ have y as a zero. Since y was arbitrary, $r_Q(P)$ must be the zero polynomial in the ring $\mathbb{Z}[P,Q]$. By equation (14) we conclude that $M(P,Q)$ divides $f(P,Q)$ in $\mathbb{Z}[P,Q]$. □

Remark 19. In the proof of Theorem 18 having fixed a nonzero value y for Q we could have made the additional requirement on the integer value x for P that it be prime to y. Thus, it is enough to have Theorem 3 hold in the regular case to imply Theorem 18, which in turn implies Theorem 3 in full generality.

The referee's computations also seemed to indicate the polynomial version in $\mathbb{Z}[P,Q]$ of Theorem 3 held for the case $p = 2$ whenever k is a multiple of 4. Theorem 3 does not consider the case $p = 2$, as the Wolstenholme congruence itself does not even hold modulo p^2, when $p = 2$. However, we can easily prove the referee's observation is true when $4 \mid k$. It is actually true for the higher modulus $U_p^3 V_p/P$. Thus, we make this an additional theorem.

Theorem 20. *Suppose $\{U,V\}$ is a pair of Lucas sequences with parameters P and Q, $k \geq 0$ is an integer divisible by 4 and $p = 2$. Then the congruence*

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{U_p^3 V_p/P},$$

holds in the ring $\mathbb{Z}[P,Q]$.

Proof. Since $U_2^3V_2/P = P^2(P^2-2Q)$, the congruence to verify becomes for $p=2$

$$U_{2k+1} \equiv Q^k \pmod{P^2(P^2-2Q)}.$$

Putting $k=4n$, we proceed by induction on n. The congruence holds true for $n=0$ and $n=1$ as is easily checked. For $n=1$, we obtain $U_9 - Q^4 = P^2(P^6 - 7P^4Q + 15P^2Q^2 - 10Q^3)$ and, using $P^2 \equiv 2Q \pmod{P^2-2Q}$, we see that the factor

$$P^6 - 7P^4Q + 15P^2Q^2 - 10Q^3 \equiv (8 - 28 + 30 - 10)Q^3 = 0 \pmod{P^2-2Q}.$$

The linear recurrent sequence (U_{8n+1}) satisfies

$$U_{8(n+2)+1} = V_8 U_{8(n+1)+1} - Q^8 U_{8n+1}, \tag{15}$$

for all $n \geq 0$. Now

$$V_8 - 2Q^4 = P^2(P^6 - 8P^4Q + 20P^2Q^2 - 16Q^3),$$

and the factor $P^6 - 8P^4Q + 20P^2Q^2 - 16Q^3$, using $P^2 \equiv 2Q \pmod{P^2-2Q}$, is seen to be congruent to $(8 - 32 + 40 - 16)Q^3 = 0$ modulo $P^2 - 2Q$. Thus, assuming $U_{8n+1} \equiv Q^{4n}$ and $U_{8(n+1)+1} \equiv Q^{4n+4}$ modulo P^2-2Q, we obtain inductively by (15) that

$$U_{8(n+2)+1} \equiv 2Q^4 \cdot Q^{4n+4} - Q^8 \cdot Q^{4n} = Q^{4(n+2)} \pmod{P^2(P^2-2Q)},$$

proving the claim. □

We remark that if $k = 1$, 2 and 3, the $\mathbb{Z}[P,Q]$-congruence of Theorem 20 does not hold even when degrading the modulus to $U_2^2V_2/P$. However, to complete the picture we can prove, using the line of proof of Theorem 20, the following proposition.

Proposition 21. *Suppose $\{U,V\}$ is a pair of Lucas sequences with parameters P and Q and $p=2$. Then the congruence*

$$\binom{(k+1)p-1}{p-1}_U \equiv Q^{kp(p-1)/2} \pmod{M(P,Q)},$$

holds in the ring $\mathbb{Z}[P,Q]$, where

$$M(P,Q) = \begin{cases} P^2 - 2Q = U_2V_2/P, & \text{if } k = 4n+1; \\ P^2 = U_2^2 = U_2^3/P, & \text{if } k = 4n+2. \end{cases}$$

5 Acknowledgments

As mentioned in the introduction, H. Ohtsuka took the pleasant initiative of sending me the unpublished solution of his Fibonacci Quarterly problem H-737 a few years ago. Part of the proof of Theorem 3 we chose to write is a direct extension of his technique. Elif Tan kindly carried out some of the numerical computations made to contend that Theorem 3 held when $U(P,Q)$ is not a regular sequence. We thank the referee for his interest and valuable questions which were addressed in Section 4.

References

[1] M. Abouzaid, Les nombres de Lucas et Lehmer sans diviseur primitif, *J. Théor. Nombres Bordeaux* **18** (2006), 299–313.

[2] G. Andrews, q-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher, *Discrete Math.* **204** (1999), 15–25.

[3] C. Ballot, A Lucas type congruence with Fibonomials (solution to advanced problem H-737), *Fibonacci Quart.* **53** (2015) 94–95, 191.

[4] C. Ballot, The congruence of Wolstenholme for generalized binomial coefficients related to Lucas sequences, *J. Integer Sequences*, **18** (2015), Article 15.5.4.

[5] C. Ballot, Lucasnomial Fuss-Catalan numbers and related divisibility questions, *J. Integer Sequences*, **21** (2018), Article 18.6.5.

[6] C. Ballot, The p-adic valuation of Lucas sequences when p is a special prime, *Fibonacci Quart.* **57** (2019) 265–275, 366.

[7] Y. Bilu, G. Hanrot, and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte, *J. Reine Angew. Math.* **539** (2001), 75–122.

[8] V. Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, and E. Jacobsthal. On the divisibility of the difference between two binomial coefficients. Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, pp. 42–54. Johan Grundt Tanums Forlag, Oslo, 1952.

[9] J. W. L. Glaisher, Congruences relating to the sums of products of the first n numbers and to other sums of products, *Quart. J. Math.* **31** (1900), 1–35.

[10] J. W. L. Glaisher, On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus p^2 or p^3, *Quart. J. Math.* **31** (1900), 321–353.

[11] Robert C. Johnson, Fibonacci numbers and matrices, preprint, 2009. Available at http://www.maths.dur.ac.uk/~dma0rcj/PED/fib.pdf.

[12] W. Kimball and W. Webb, A congruence for fibonomial coefficients modulo p^3, *Fibonacci Quart.* **33** (1995) 290–297.

[13] W. Kimball and W. Webb, Some congruences for generalized binomial coefficients, *Rocky Mountain J. Math.* **25** (1995) 1079–1085.

[14] W. Kimball and W. Webb, Some generalizations of Wolstenholme's theorem, in *Applications of Fibonacci Numbers* **8**, Kluwer Acad. Publ., 1999, pp. 213–218.

[15] W. Kimball and W. Webb, Congruence properties of Fibonacci numbers and Fibonacci coefficients modulo p^2. *Applications of Fibonacci Numbers* **5**, Kluwer Acad. Publ., 1993, pp. 399–403.

[16] É. Lucas, Théorie des fonctions simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[17] É. Lucas, *Théorie des Nombres*, Éditions Jacques Gabay, 1991.

[18] H. Ohtsuka, Problem H-737, *Fibonacci Quart.* **51** (2013), 186.

[19] Ling-Ling Shi, Congruences for Lucas u-nomial coefficients modulo p^3, *Rocky Mountain J. Math.* **37** (2007), 1027–1042.

[20] H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Math. Soc. Series of Monographs and Advanced Texts, Wiley, 1998.

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

2010 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B65, 11B39.
Keywords: generalized binomial coefficient, Wolstenholme's congruence, Lucas sequence, rank of appearance.

Received August 9 2019; revised version received December 19 2019; December 24 2019; March 11 2020. Published in *Journal of Integer Sequences*, March 17 2020.

Return to Journal of Integer Sequences home page.