Journal of Integer Sequences, Vol. 18 (2015),
Article 15.5.4

The Congruence of Wolstenholme for Generalized Binomial Coefficients Related to Lucas Sequences

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

Abstract

In recent years much research has been carried out on extending Wolstenholme classical congruence modulo the cube of a prime to higher prime powers. Here we show that this work can be done in much broader generality by replacing ordinary binomials by Lucasnomials, which are generalized binomial coefficients related to fundamental Lucas sequences. The paper builds on earlier work of Kimball and Webb in relation to the Fibonacci sequence and on recent work of the author related to congruences involving sums of quotients of Lucas sequences. The paper offers what may be a surprising line of development for very classical congruences.

1 Introduction

In 1862 Wolstenholme [37] established a now well-known congruence for binomial coefficients, namely

Theorem 1. *Let p be a prime number ≥ 5. Then*

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

Babbage [1], in 1819, had actually shown that congruence (1) held modulo p^2 for all primes p greater than 2. There is a survey paper [24] on the numerous generalizations of Theorem 1 discovered since the paper of Wolstenholme appeared in 1862. This survey also contains many other related results.

We focus first our attention on the sligthly more general congruence

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

which holds for all primes $p \geq 5$ and all nonnegative integers k. According to the survey [24], congruence (2) was proved in 1900 by Glaisher [12, p. 21], [13, p. 33].

If $A = (A_n)_{n\geq 0}$ is a sequence of complex numbers where $A_0 = 0$ and all $A_n \neq 0$ for $n > 0$, then one defines, for m and n nonnegative integers, the *generalized* binomial coefficient

$$\binom{m}{n}_A = \begin{cases} \frac{A_m A_{m-1} \ldots A_{m-n+1}}{A_n A_{n-1} \ldots A_1}, & \text{if } m \geq n \geq 1; \\ 1, & \text{if } n = 0; \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

The well-written paper [14] contains a number of early references about these coefficients and investigated several of their general properties. We point out another early reference [34], not often quoted, in which Ward gives two equivalent criteria that imply the integrality of the generalized coefficients $\binom{m}{n}_A$ of a sequence of integers A. One of them is that A be a *strong divisibility sequence*, i.e., one for which $A_{\gcd(m,n)} = \gcd(A_m, A_n)$ for all $m > n > 0$; the other criterion is expressed in terms of ranks of appearance of prime powers in A. The *rank of appearance* $\rho = \rho_A(x)$ of a nonzero integer x with respect to A is, if it exists, the least positive integer t such x divides the integer A_t. The equivalence of the two criteria of Ward was essentially rediscovered in [21]. When A is the Fibonacci sequence $F = (F_n)_{n\geq 0}$, defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$, these binomial coefficients are called *Fibonomials*. Many papers have studied their properties.

Kimball and Webb [19, Lemma 3] proved an analogue of the Wolstenholme-Glaisher congruence (2), which we rewrite as a theorem below.

Theorem 2. *Let p be a prime at least 7 whose rank of appearance ρ in the Fibonacci sequence is of the form $p - \epsilon_p$, where ϵ_p is ± 1. Then for all integers $k \geq 0$*

$$\binom{(k+1)\rho-1}{\rho-1}_F \equiv \epsilon_p^k \pmod{p^3}, \tag{4}$$

where the symbol $\binom{*}{*}_F$ stands for the Fibonomial coefficient.

Some papers have considered the generalized binomial coefficients when A is a fundamental Lucas sequence, that is, a sequence $U = U(P, Q)$ satisfying

$$U_0 = 0,\ U_1 = 1 \ \text{ and } U_{n+2} = PU_{n+1} - QU_n, \ \text{ for all } n \geq 0, \tag{5}$$

where (P,Q) is a pair of integers, Q nonzero. We will refer to these generalized binomials as *Lucasnomial* coefficients, or *Lucasnomials*, in the sequel. Ordinary binomials are Lucasnomial coefficients with parameters $(P,Q) = (2,1)$, whereas the Fibonomials correspond to $(P,Q) = (1,-1)$. Thus it makes sense to look for a simple congruence for the general Lucasnomial

$$\binom{(k+1)\rho-1}{\rho-1}_U \pmod{p^3}, \tag{6}$$

valid for an arbitrary Lucas sequence U, that would encompass both the congruence (2) and Theorem 2.

Here ρ represents the rank of appearance of the prime p in U. It is known to exist for all primes p not dividing Q and, for p odd, to divide $p - \epsilon_p$, where ϵ_p is the Legendre character $(D \mid p)$ and D is $P^2 - 4Q$. To obtain a congruence modulo p^3 it is necessary to require, as in Theorem 2, that the rank ρ be maximal, i.e., be equal to $p - \epsilon_p$. Note that the rank of any prime p is maximal and equal to p for $U_n = n$ ($D = 0$, $\epsilon_p = 0$). However, the case $\epsilon_p = 0$ only occurs for $p = 5$ for the Fibonacci sequence $F = U(1,-1)$, a case that Theorem 2 does not address. A calculation for $p = 5$ yields

$$\binom{2\rho-1}{\rho-1}_F = \binom{9}{4}_F \equiv 1 \pmod{125}. \tag{7}$$

This residue of 1 at least conforms to what one gets in (2), but does not match the expression ϵ_p^k of Theorem 2 which would yield 0.

Thus, one needs to generalize the results of the paper [19] from Fibonomial coefficients to Lucasnomial coefficients and include the case $\epsilon_p = 0$ in the analysis. However, some of the results leading to Theorem 2 in [19] seem, at first sight, to depend on idiosyncracies of the Fibonacci sequence. Thus, a few numerical calculations helped us believe in the existence of a generalization and were useful in guiding us to it.

Theorem 3. *Let $U = U(P,Q)$ be a fundamental Lucas sequence with parameters P and Q. Let $p \geq 5$, $p \nmid Q$, be a prime whose rank of appearance ρ in U is equal to $p - \epsilon_p$, where ϵ_p is the Legendre character $(D \mid p)$, $D = P^2 - 4Q$. Then for all integers $k \geq 0$*

$$\binom{(k+1)\rho-1}{\rho-1}_U \equiv (-1)^{k\epsilon_p} Q^{k\rho(\rho-1)/2} \pmod{p^3}, \tag{8}$$

where the symbol $\binom{*}{*}_U$ stands for the Lucasnomial coefficient.

Remark 4. Theorem 3 implies that for all $k \geq 0$

$$\binom{(k+1)\rho-1}{\rho-1}_U \equiv \binom{2\rho-1}{\rho-1}_U^k \pmod{p^3}.$$

Remark 5. Congruence (2), Theorem 2 and, as readily checked, congruence (7) are implied by Theorem 3. Indeed, the sequence $A_n = n$ is $U_n(2,1)$, for which $Q = 1$ and $\epsilon_p = 0$ for all primes. To see that Theorem 2 is a corollary of Theorem 3, it suffices to check that

$$\epsilon_p = -(-1)^{\rho(\rho-1)/2},$$

for every odd prime $p > 5$ of maximal rank in the Fibonacci sequence $U(1,-1)$. All primes of rank $p \pm 1$ in the Fibonacci sequence must be congruent to $3 \pmod 4$, since by Euler's criterion for Lucas sequences (19) we need to have $(-1 \mid p) = -1$. If $\epsilon_p = 1$, that is, if $\rho = p-1$, then $\rho(\rho-1) \equiv 2 \pmod 4$ so that $-(-1)^{\rho(\rho-1)/2} = +1 = \epsilon_p$. If $\epsilon_p = -1$, that is, $\rho = p+1$, then $\rho(\rho-1) \equiv 0 \pmod 4$ so $-(-1)^{\rho(\rho-1)/2} = -1 = \epsilon_p$.

Remark 6. Although throughout the paper we assume rank maximality, not all is lost when a prime does not have maximal rank. As will be easily inferred from the proof of Theorem 3, we have for general rank a weaker congruence albeit valid for all $p \geq 3$ which we state below.

Theorem 7. *If a prime $p \geq 3$, $p \nmid Q$, has rank ρ in $U(P,Q)$, then for all integers $k \geq 0$*

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

Remark 8. Various other Lucasnomial generalizations of the Glaisher congruence (2), besides Theorems 3 and 7, are possible. For one instance, retaining p instead of ρ in the terms of the congruence but replacing p in the modulus by U_p, we can prove the theorem.

Theorem 9. *Suppose $U(P,Q)$ is a fundamental Lucas sequence with P and Q coprime and $U_2U_3U_4U_6$ nonzero. Let $p \geq 5$ be a prime. Then for all $k \geq 0$ we have the congruence*

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

When U_p is a prime then p is the rank of U_p so that, in that case, Theorem 9 follows from Theorem 7. For $U(1,-1)$, the Fibonacci sequence, the congruence in Theorem 9 may be deduced from the statement of a problem posed by Ohtsuka [26]. Generalizing the published solution to this problem [4], one can derive Theorem 9.

Section 2 of the paper is devoted to some relevant additional remarks on Lucas sequences, some useful lemmas and to proofs of Theorem 3 and Theorem 7.

For all primes $p \geq 5$ and all nonnegative integers k and ℓ, we have the congruence

$$\binom{kp}{\ell p} \equiv \binom{k}{\ell} \pmod{p^3}. \tag{9}$$

This congruence supersedes congruence (2) and was first proved in a collective paper [10] which appeared in 1952. It was reproved by Bailey some forty years later in the paper

[2], where the case $(k, \ell) = (2, 1)$, which is equivalent to Wolstenholme's congruence (1), is proved first before an induction on k yielded congruence (2) and another proof by induction gave (9). Interestingly another simple argument, combinatorial, reduces the proof of (9) to that of the case $(k, \ell) = (2, 1)$ in the book [31, solution of exercise 1.14, p. 165].

Similarly in [19], Theorem 2 is used by the authors to produce an analogue of (9) for the Fibonacci sequence $U = F$. That is, in our notation, for primes $p \geq 7$ of rank $\rho = p - \epsilon_p$, where $\epsilon_p = \pm 1$, their result [19, p. 296] states that

$$\binom{k\rho}{\ell\rho}_F \equiv \epsilon_p^{(k-\ell)\ell} \binom{k}{\ell}_{F'} \pmod{p^3}, \tag{10}$$

where $F'_t = F_{\rho t}$ for all $t \geq 0$, k, ℓ are integers satisfying $k \geq \ell \geq 1$. Section 3 states and proves a congruence, Theorem 13, for Lucasnomials $\binom{k\rho}{\ell\rho}_U \pmod{p^3}$ that subsumes the congruences (9) and (10). Here again the proof of this more general result is easily derived from Theorem 3. We raise in passing the question of the existence of a combinatorial argument that would reduce Theorem 13 to the case $(k, \ell) = (2, 1)$. Lucasnomial coefficients received two distinct combinatorial interpretations in the paper [30], both of which were explained another time in [8]. Also a q-analogue of (9) that uses q-binomial coefficients was established in the paper [32].

In the fourth section, we selected three congruences for binomials $\binom{2p-1}{p-1} \pmod{p^5}$, namely (25), (26) and (27), and establish for each a generalization to Lucasnomial coefficients $\binom{2\rho-1}{\rho-1}_U \pmod{p^5}$ for primes $p \geq 7$ of maximal rank ρ in U. Not to lengthen an already long introduction we only state the example of congruence (27), i.e.,

$$\binom{2p-1}{p-1} \equiv 1 - p^2 \sum_{0<t<p} \frac{1}{t^2} \pmod{p^5},$$

which generalizes into

$$\binom{2\rho-1}{\rho-1}_U \equiv (-1)^{\rho-1} Q^{\frac{\rho(\rho-1)}{2}} \left(1 - 4\frac{U_\rho^2}{V_\rho^2} \sum_{0<t<\rho} \frac{Q^t}{U_t^2}\right) \pmod{p^5},$$

where $U(P, Q)$ is a fundamental Lucas sequence and V its companion Lucas sequence. The V sequence is defined by $V_0 = 2$, $V_1 = P$ and the same recursion, $V_{n+2} = PV_{n+1} - QV_n$ for all $n \geq 0$, as the U sequence. Thus, the companion Lucas sequence of $U_n(2, 1) = n$ is $V_n(2, 1) = 2$, for all $n \geq 0$. At the basis of these results are congruences modulo a prime p or modulo p^2 for generalized harmonic sums $\sum_{t=1}^{\rho-1} (V_t/U_t)^\nu$ which are compiled in Lemma 10. We recall that Theorem 1 is intimately linked with the congruence $\sum_{t=1}^{p-1} 1/t \equiv 0 \pmod{p^2}$ for primes $p \geq 5$.

Note that the condition that p be of maximal rank in U may be viewed as a quadratic analogue of Artin's conjecture which gives a positive density (equal to a positive rational number times Artin's constant) for the set of primes p for which a given a is a primitive root (mod p), when a is a non-square integer and $|a| \geq 2$. Hooley [17] proved Artin's conjecture conditionally to some generalized Riemann hypotheses. So did Roskam [28, 29] for the set of primes p for which a fundamental unit of a quadratic field has maximal order modulo (p). Thus, given $U(P, Q)$, Q not a square, our theorems presumably should also concern sets of primes of positive densities.

In recent years congruences for ordinary binomials $\binom{2p-1}{p-1} \pmod{p^e}$ have been established for larger and larger exponents e [24, pp. 4–6]. No doubt there must be higher corresponding congruences for Lucasnomials. In fact, we end Section 4 with such a congruence, expressed in Theorem 28, when $e = 6$. Generalizations of (25) are stated in Theorems 20 and 27, those of (26) and the above congruence (27) appear in Theorems 21 and 24 respectively. We added an appendix as a short fifth section where the integrality of all Lucasnomial coefficients $\binom{m}{n}_U$ is asserted for all U Lucas sequences, including degenerate cases, provided we make a reasonable amendment to the definition (3).

Familiarity with Lucas sequences is assumed throughout the paper, but the reader may want to consult the introduction of [7] and the references it mentions. Chapter 4 of the book [36] is a useful introduction to these sequences.

Lucasnomial coefficients have already been the object of generalizations of classical arithmetic properties of ordinary binomial coefficients. Kummer's theorem giving the exact power of a prime p in the binomial coefficient $\binom{m+n}{n}$ as the number of carries in the addition of m and n in radix p was extended to generalized binomials $\binom{m+n}{n}_A$, when A is a strong divisibility sequence of positive integers [21]. That includes, in particular, all Lucas sequences $U(P, Q)$ with positive terms when P and Q are coprime. A further Kummer rule pertaining to generalized binomials $\binom{*}{*}_U$, valid for an arbitrary nondegenerate fundamental U Lucas sequence, appears in the preprint [3].

Also various generalizations of the celebrated theorem of Lucas:

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

where r and s are nonnegative integers less than the prime p, were achieved in terms of Lucasnomials $\binom{mp+r}{np+s}_U$, often under restrictive hypotheses on the Lucas sequence $U(P, Q)$ [35, 16, 18].

In fact both the theorems of Kummer and of Lucas had been generalized in an earlier paper [11] but with respect to q-binomial coefficients.

2 Preliminaries and a proof of Theorem 3

Lucas theory is often developed with the two hypotheses that $U(P, Q)$ is nondegenerate and $\gcd(P, Q)$ is 1. The Lucas sequence $U(P, Q)$ is called *degenerate* whenever the ratio of the zeros α and β of $x^2 - Px + Q$ is a root of unity. We do not make any of these assumptions here. If U is degenerate then we must have $U_2U_3U_4U_6 = 0$. Indeed, if $\alpha \neq \beta$ then $U_t = \frac{\alpha^t - \beta^t}{\alpha - \beta}$ and the ratio α/β, lying in the quadratic field $\mathbb{Q}(\sqrt{D})$, must be a second, third, fourth or sixth root of unity. Thus, some terms of the sequence U will be 0, but rather than discard those Lucas sequences from our analysis, we make a small amendment to the definition (3) to ensure that the corresponding Lucasnomials $\binom{m}{n}_U$ are well-defined as rational numbers. Although the hypotheses of Theorems 3 and 13 or of the theorems of Section 4 if applied to a prime $p \geq 11$ prevent the corresponding Lucasnomials from having zero terms, this is not necessarily the case if $p = 5$ or $p = 7$. With $\gcd(P, Q) > 1$, the Lucas sequence $A = U(P, Q)$ is no longer a strong divisibility sequence. Nevertheless A, or λA, λ an integer, satisfies some 'convexity' property. Namely for all prime powers p^a ($a \geq 1$), $p \nmid Q$, and for all x and $y \geq 1$, we have

$$\#\,\{t \in [x+y],\ p^a \mid A_t\} \ \geq\ \#\,\{t \in [x],\ p^a \mid A_t\} + \#\,\{t \in [y],\ p^a \mid A_t\}. \tag{11}$$

Here, if z is an integer ≥ 1, $[z]$ denotes the set of natural numbers $1, 2, \ldots, z$. This property holds because for such prime powers p^a, we have $p^a \mid U_t$ iff $\rho(p^a) \mid t$, where $\rho(p^a)$ is the rank of appearance of p^a in U, and because $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$ for all real numbers x and y.

The convention we adopt for the generalized binomials $\binom{m}{n}_A$ of definition (3) is that if there are zero terms in the product $\prod_{i=1}^{n} \frac{A_{m+1-i}}{A_i}$ then

a 0 in the numerator and a 0 in the denominator **cancel out** as a 1. (12)

With convention (12), property (11) satisfied by $A = \lambda U$, for all Lucas sequences U, guarantees that the generalized binomial $\binom{m}{n}_A$ is a well-defined rational number. Indeed this property implies that the number of 0 terms in the numerator of $\prod_{i=1}^{n} \frac{A_{m+1-i}}{A_i}$ is at least that of its denominator. It also implies that $\binom{m}{n}_A$, m and n nonnegative integers, has nonnegative p-adic valuation for all primes $p \nmid Q$. In fact we can show it is always a rational integer. [1]

As already mentioned, to each fundamental Lucas sequence $U(P, Q)$ we associate a *companion* Lucas sequence $V = V(P, Q)$ which obeys recursion (5), but has initial values $V_0 = 2$ and $V_1 = P$. The following identities are all classical ones and are all valid no matter what the value of $\gcd(P, Q)$ is. We will use them throughout the paper.

$$\begin{aligned}
2U_{s+t} &= U_sV_t + U_tV_s, && (13)\\
2V_{s+t} &= V_sV_t + DU_sU_t, && (14)\\
V_t^2 - DU_t^2 &= 4Q^t, && (15)\\
U_{2t} &= U_tV_t, && (16)\\
V_{2t} &= V_t^2 - 2Q^t, && (17)\\
2Q^tU_{s-t} &= U_sV_t - U_tV_s. && (18)
\end{aligned}$$

[1] See our short Appendix.

We referred to Euler's criterion for Lucas sequences in our introduction. The criterion states that

$$p \mid U_{(p-\epsilon_p)/2} \text{ iff } Q \text{ is a square modulo } p, \tag{19}$$

where $U(P,Q)$ is a fundamental Lucas sequence and p is a prime that does not divide $2DQ$ [36, pp. 84–85].

Note that our theorems and the lemmas of Section 4 all deal with primes $p \geq 5$ of maximal rank. In their statements, we sometimes omit to mention the condition $p \nmid Q$, because that condition is necessary. Indeed, if $p \mid Q$, then, by (5), $U_t \equiv P^{t-1} \pmod{p}$. Thus, p has no rank, because if p divided P, then $\rho(p)$ would be equal to 2, as $U_2 = P$, a contradiction.

Given a prime p of rank ρ and a nonnegative integer ν, we write

$$\Sigma_\nu := \sum_{0<t<\rho} \frac{V_t^\nu}{U_t^\nu} \text{ and } \Sigma_{1,1} := \sum_{0<s<t<\rho} \frac{V_s V_t}{U_s U_t}. \tag{20}$$

The proof of Theorem 3 we are about to write uses a few lemmas which we state first.

Lemma 10. *Let (U,V) be a pair of Lucas sequences with parameters P and Q. Let ν be a nonnegative integer. If $p \nmid Q$ is a prime at least $\nu+3$ of maximal rank ρ, i.e., of rank $p-\epsilon_p$, where $\epsilon_p = 0$ or ± 1, then* [2]

$$\Sigma_\nu \equiv \begin{cases} 0 \pmod{p^2}, & \text{if } \nu \text{ is odd;} \\ 0 \pmod{p}, & \text{if } \epsilon_p = -1 \text{ or } 0; \\ -2D^{\nu/2} \pmod{p}, & \text{if } \nu \text{ is even and } \epsilon_p = 1. \end{cases} \tag{21}$$

Moreover, if p is an odd prime not dividing Q of any rank ρ, then

$$\Sigma_\nu \equiv 0 \pmod{p}, \quad \text{for all odd } \nu. \tag{22}$$

Proof. The case ν odd of (21) is Theorem 3 of [5]. (The case $\nu = 1$ first appeared, nearly complete, as the main theorem of the paper [20], but also, nearly, as a corollary of the main theorem of [27], and as a particular case of [6, Thm. 4.1], or of [7, Thms. 3 and 12].)

The case ν even can be treated with the very same arguments used in the last part of the proof of Theorem 4 of [5, p. 5]. (The basic facts, noted first in [20], are that, by (18), all V_t/U_t are distinct $\pmod{p}$ for $t \in (0,\rho)$ and no V_t/U_t is $\pm\sqrt{D} \pmod{p}$ by (15); also $p \mid \sum_{t=1}^{p} t^e$ if $p-1 \nmid e$). The condition $p \geq \nu+3$ is a sufficient condition which guarantees that $p-1 \nmid \nu$ for $\nu \geq 2$ even.

The additional congruence (22) for ν odd, but without the restrictions that ρ be maximal and $p \geq \nu+3$, is a consequence of the congruence $\pmod{p^2}$ on the sixth line of the proof of Theorem 4 of [5, p. 4]. □

[2] unless $\nu = 0$ and $\epsilon_p = 0$, when $\Sigma_0 \equiv -1 \pmod{p}$.

Lemma 11. *Let (U, V) be a pair of Lucas sequences with parameters P and Q. If $p \nmid 6Q$ is a prime of maximal rank ρ in U, then*

$$\Sigma_{1,1} \equiv \begin{cases} 0 \pmod{p}, & \text{if } \epsilon_p = 0 \text{ or } -1; \\ D \pmod{p}, & \text{if } \epsilon_p = 1. \end{cases}$$

Proof. We have $\Sigma_1^2 = \Sigma_2 + 2\Sigma_{1,1}$ so that $\Sigma_{1,1} \equiv -\frac{1}{2}\Sigma_2 \pmod{p}$, since, by Lemma 10, p^4 divides Σ_1^2 and Σ_2 is either 0 or $-2D \pmod{p}$. □

Lemma 12. *Let $V = V(P, Q)$ be a companion Lucas sequence. Let $p \nmid Q$ be an odd prime of rank ρ and $t \geq 0$ an integer. Then modulo p^2 we have*

$$V_{t\rho} \equiv \begin{cases} 2Q^{t\rho/2}, & \text{if } t \text{ is even;} \\ -2Q^{t\rho/2}, & \text{if } t \text{ is odd and } \rho \text{ is even.} \end{cases}$$

Proof. Assume t is even. By (15), $V_{t\rho/2}^2 \equiv 4Q^{t\rho/2} \pmod{p^2}$ since p divides $U_{t\rho/2}$. However, by (17), $V_{t\rho} = V_{t\rho/2}^2 - 2Q^{t\rho/2} \equiv 2Q^{t\rho/2} \pmod{p^2}$.

Suppose t odd and ρ even. Since p divides $U_{t\rho}$, but not $U_{t\rho/2}$, we see by (16) that p divides $V_{t\rho/2}$. So by (17) we find that $V_{t\rho} \equiv -2Q^{t\rho/2} \pmod{p^2}$. □

We are now ready for a proof of Theorem 3.

Proof. We have

$$\binom{(k+1)\rho - 1}{\rho - 1}_U = \frac{\prod_{t=1}^{\rho-1} U_{k\rho+t}}{\prod_{t=1}^{\rho-1} U_t}.$$

By the addition formula (13), we find that

$$\begin{aligned} 2^{\rho-1}\prod_{t=1}^{\rho-1} U_{k\rho+t} &= \prod_{t=1}^{\rho-1}(V_{k\rho}U_t + U_{k\rho}V_t) \\ &\equiv (V_{k\rho}^{\rho-1} + V_{k\rho}^{\rho-2}U_{k\rho}\Sigma_1 + V_{k\rho}^{\rho-3}U_{k\rho}^2\Sigma_{1,1}) \times \prod_{t=1}^{\rho-1} U_t \qquad (23) \\ &\equiv (V_{k\rho}^{\rho-1} + V_{k\rho}^{\rho-3}U_{k\rho}^2\Sigma_{1,1}) \times \prod_{t=1}^{\rho-1} U_t \pmod{p^3}, \end{aligned}$$

since p divides $U_{k\rho}$ and, by Lemma 11, Σ_1 is $0 \pmod{p^2}$.

We first examine the cases ρ is $p + 1$ and ρ is p. In those cases $U_{k\rho}^2\Sigma_{1,1}$ is $0 \pmod{p^3}$ by Lemma 11. Hence,

$$\binom{(k+1)\rho - 1}{\rho - 1}_U \equiv \left(\frac{V_{k\rho}}{2}\right)^{\rho-1} \pmod{p^3}.$$

If ρ is p, then, by (15) and the fact that $p^3 \mid DU_{k\rho}^2$, we see that $V_{k\rho}^2 \equiv 4Q^{k\rho} \pmod{p^3}$. Therefore,

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

yielding the result in that case. Suppose ρ is $p+1$. By Lemma 12 there is an integer, or a half-integer, λ such that $\frac{V_{k\rho}}{2} = (-1)^k Q^{k\rho/2} + \lambda p^2$. Raising both members of the previous equation to the pth power gives $(V_{k\rho}/2)^p \equiv (-1)^k Q^{k\rho p/2} \pmod{p^3}$. But $(-1)^k = (-1)^{-k} = (-1)^{k\epsilon_p}$ so the theorem follows.

Suppose now ϵ_p is 1, that is, ρ is $p-1$. By Lemma 11, $\Sigma_{1,1} \equiv D \pmod{p}$ so that $U_{k\rho}^2 \Sigma_{1,1} \equiv DU_{k\rho}^2 \pmod{p^3}$. But, by (15), $DU_{k\rho}^2 = V_{k\rho}^2 - 4Q^{k\rho}$. Therefore, we have

$$2^{\rho-1}\binom{(k+1)\rho-1}{\rho-1}_U \equiv 2V_{k\rho}^{\rho-1} - 4Q^{k\rho}V_{k\rho}^{\rho-3} \pmod{p^3}.$$

This gives

$$\begin{aligned} \binom{(k+1)\rho-1}{\rho-1}_U &\equiv \left(\frac{V_{k\rho}}{2}\right)^p \cdot \alpha_{p,k} \pmod{p^3}, \\ \text{with} \qquad \alpha_{p,k} &:= 2\left(\frac{2}{V_{k\rho}}\right)^2 - Q^{k\rho}\left(\frac{2}{V_{k\rho}}\right)^4. \end{aligned}$$

By Lemma 12, $V_{k\rho}/2 \equiv (-1)^k Q^{k\rho/2} \pmod{p^2}$. Raising the previous congruence to the pth power yields $(V_{k\rho}/2)^p \equiv (-1)^k Q^{kp\rho/2} \pmod{p^3}$, while inverting it yields the existence of an integer μ such that $2/V_{k\rho} \equiv (-1)^k Q^{-k\rho/2} + \mu p^2 \pmod{p^3}$. Thus, we find that, modulo p^3,

$$\begin{aligned} \alpha_{p,k} &\equiv 2\big((-1)^k Q^{-k\rho/2} + \mu p^2\big)^2 - Q^{k\rho}\big((-1)^k Q^{-k\rho/2} + \mu p^2\big)^4 \\ &\equiv (2Q^{-k\rho} + (-1)^k 4Q^{-k\rho/2}\mu p^2) - Q^{k\rho}(Q^{-2k\rho} + (-1)^k 4Q^{-3k\rho/2}\mu p^2) \\ &= Q^{-k\rho}. \end{aligned}$$

Thus, we end up with

$$\binom{(k+1)\rho-1}{\rho-1}_U \equiv (-1)^k Q^{kp\rho/2} Q^{-k\rho} = (-1)^{k\epsilon_p} Q^{k\rho(p-2)/2} \pmod{p^3},$$

which yields the theorem. □

The above proof is the first that came to us. It proceeds case by case according to whether the value of the rank of p is $p+1$, p or $p-1$ and, thus, appears somewhat miraculous. Although we initially wrote case by case proofs for the higher congruences of Section 4, we ended up presenting a global and thus less seemingly miraculous approach at least for Theorems 21 and 24.

We now prove Theorem 7 using the elements of the proof of Theorem 3.

Proof of Theorem 7. Since, in (23), $U_{k\rho}$ is $0 \pmod p$ and, by (22), Σ_1 is also $0 \pmod p$, we find that for all primes $p \geq 3$

$$\binom{(k+1)\rho-1}{\rho-1}_U \equiv \left(\frac{V_{k\rho}}{2}\right)^{\rho-1} \pmod{p^2}.$$

By (15), $(V_{k\rho}/2)^2 \equiv 4Q^{k\rho}/4 = Q^{k\rho} \pmod{p^2}$. Thus, if ρ is odd, then $(V_{k\rho}/2)^{\rho-1} \equiv \left(Q^{k\rho}\right)^{(\rho-1)/2} = (-1)^{k(\rho-1)}Q^{k\rho(\rho-1)/2} \pmod{p^2}$. If k is even, then, by Lemma 12, $V_{k\rho}/2 \equiv Q^{k\rho/2} \pmod{p^2}$ and the result holds by raising the congruence to the power $\rho-1$. If k is odd and ρ even, then, again by Lemma 12, $V_{k\rho}/2 \equiv -Q^{k\rho/2} = (-1)^k Q^{k\rho/2} \pmod{p^2}$, which raised to the power $\rho - 1$ yields the theorem. □

3 Lucasnomials $\binom{k\rho}{\ell\rho}_U \pmod{p^3}$

Here is our common generalization of the Ljunggren et al. congruence (9) and Kimball and Webb's theorem (10).

Theorem 13. *Let U, V be a pair of Lucas sequences with parameters P and Q. Let $p \geq 5$, $p \nmid Q$, be a prime whose rank of appearance ρ is $p \pm 1$ or p. Then, for all nonnegative integers k and ℓ, we have*

$$\binom{k\rho}{\ell\rho}_U \equiv \left((-1)^{\rho-1}Q^{\rho(\rho-1)/2}\right)^{\ell(k-\ell)} \binom{k}{\ell}_{U'} \pmod{p^3}, \tag{24}$$

where U' is the sequence $U_\rho \times U(V_\rho, Q^\rho)$.

Proof. Note that if ρ is maximal, then the factor $(-1)^{\epsilon_p}$ of Theorem 3 may be replaced by $(-1)^{\rho-1}$. We only need a proof in case $k > \ell \geq 1$. With convention (12) we may write

$$\begin{aligned}
\binom{k\rho}{\ell\rho}_U &= \frac{U_{k\rho}U_{k\rho-1}\cdots U_{(k-\ell)\rho+1}}{U_{\ell\rho}U_{\ell\rho-1}\cdots U_1} \\
&= \frac{U_{k\rho}U_{(k-1)\rho}\cdots U_{(k-\ell+1)\rho}}{U_{\ell\rho}U_{(\ell-1)\rho}\cdots U_\rho} \cdot \frac{\prod_{i=k-\ell}^{k-1}\prod_{t=1}^{\rho-1} U_{i\rho+t}}{\prod_{i=0}^{\ell-1}\prod_{t=1}^{\rho-1} U_{i\rho+t}} \\
&= \binom{k}{\ell}_{U'} \cdot \frac{\prod_{i=k-\ell}^{k-1}\prod_{t=1}^{\rho-1} U_{i\rho+t}}{\left(\prod_{t=1}^{\rho-1} U_t\right)^\ell} \cdot \frac{\left(\prod_{t=1}^{\rho-1} U_t\right)^\ell}{\prod_{i=0}^{\ell-1}\prod_{t=1}^{\rho-1} U_{i\rho+t}} \\
&= \binom{k}{\ell}_{U'} \cdot \prod_{i=k-\ell}^{k-1} \binom{(i+1)\rho-1}{\rho-1}_U \cdot \left(\prod_{i=0}^{\ell-1} \binom{(i+1)\rho-1}{\rho-1}_U\right)^{-1} \\
&\equiv \binom{k}{\ell}_{U'} \cdot \binom{2\rho-1}{\rho-1}_U^{\sum_{i=k-\ell}^{k-1} i - \sum_{i=0}^{\ell-1} i} \qquad (\text{ by Remark 4 }) \\
&= \binom{k}{\ell}_{U'} \cdot \binom{2\rho-1}{\rho-1}_U^{\ell(k-\ell)} \pmod{p^3},
\end{aligned}$$

yielding, by Theorem 3, the theorem. □

Remark 14. If $p \geq 3$, $p \nmid Q$, is a prime and no assumption is made about its rank, then congruence (24) holds modulo p^2. This is established by following the proof of Theorem 13 and using Theorem 7.

Remark 15. If, in Theorem 13, $U_\rho \neq 0$ then we might as well set U' equal to $U(V_\rho, Q^\rho)$.

Remark 16. If $U = U(2,1)$, then $U_t = t$ and $U'_t = pt$, or $U'_t = t$ by the above remark. Thus the theorem implies that

$$\binom{kp}{\ell p} \equiv \binom{k}{\ell}_{U'} = \binom{k}{\ell} \pmod{p^3},$$

which is the classical congruence (9) of Ljunggren et alii. For $U = U(1,-1)$ and $\epsilon_p = \pm 1$ we saw in Remark 5 that $\epsilon_p = -(-1)^{\rho(\rho-1)/2} = -Q^{\rho(\rho-1)/2}$ so that Theorem 13 implies (10).

Since we took care of including all cases of Lucas sequences in our theorems, we provide an example of an application of Theorem 13 to a degenerate Lucas sequence.

Example 17. Consider $U(2,2)$. Its first terms are

$$0,\ 1,\ 2,\ 2,\ 0, -4, -8, -8,\ 0, 16, 32, 32,\ 0, \ldots$$

So Theorem 13 applies to $p = 5$ since its rank is maximal and equal to 4. Choose, say $k = 3$ and $\ell = 2$. By our extended definition of (3), we have $\binom{3}{2}_{U'} = 1$ and $(-1)^{\ell(k-\ell)\epsilon_p} Q^{\ell(k-\ell)\rho(\rho-1)/2} = 2^{12}$. Computing $\binom{12}{8}_U$ we may verify the congruence modulo 125, which in that case is an equality, since

$$\binom{12}{8}_U = \frac{U_{11} \cdot U_{10} \cdot U_9}{U_3 \cdot U_2 \cdot U_1} = \frac{16 \cdot 32 \cdot 32}{2 \cdot 2 \cdot 1} = 2^{12}.$$

4 Lucasnomials $\binom{2\rho-1}{\rho-1}_U \pmod{p^5}$

The congruence of Wolstenholme has been studied to prime powers higher than the third. In particular, we have, for all primes $p \geq 7$,

$$\begin{aligned} \binom{2p-1}{p-1} &\equiv 1 + p \sum_{0<t<p} \frac{1}{t} + p^2 \sum_{0<s<t<p} \frac{1}{st} \pmod{p^5} & (25)\\ &\equiv 1 + 2p \sum_{0<t<p} \frac{1}{t} \pmod{p^5} & (26)\\ &\equiv 1 - p^2 \sum_{0<t<p} \frac{1}{t^2} \pmod{p^5}. & (27) \end{aligned}$$

We will find congruences for the Lucasnomial coefficients $\binom{2\rho-1}{\rho-1}_U$, valid for a general fundamental Lucas sequence U, modulo the fifth power of a prime of maximal rank ρ, which generalize the three congruences above. Expanding the binomial $\binom{2p-1}{p-1}$, as was done more generally for Lucasnomials in the proof of Theorem 3, one falls naturally on the congruence (25). This expansion appears, for instance, in the proof of Proposition 1 in [25]. Congruence (26) is a special case of Theorem 3 of the paper [38] and was known to hold for primes $p \geq 5$ modulo p^4 much earlier, while congruence (27) appears in [23, p. 385].

Given a prime p of rank ρ we make a formal definition to complete the notation introduced in (20).

Definition 18. If $\nu \geq 1$ is an integer, then

$$\Sigma_{\nu,\cdots,\nu\ (k\text{ times})} := \sum \left(\frac{V_{t_1}}{U_{t_1}}\right)^{\nu} \cdots \left(\frac{V_{t_k}}{U_{t_k}}\right)^{\nu},$$

the sum being over all $(t_1, \ldots, t_k)$ in $(0, \rho)^k$, $t_1 < t_2 < \cdots < t_k$.

If $1 \leq \nu_1 < \nu_2$ are two integers, then $\Sigma_{\nu_1,\cdots,\nu_1,\,\nu_2,\cdots,\nu_2}$, where ν_u, $u = 1$ or 2, is respectively repeated k_u times, is defined as

$$\sum \left(\frac{V_{t_1}}{U_{t_1}}\right)^{\nu_1} \cdots \left(\frac{V_{t_{k_1}}}{U_{t_{k_1}}}\right)^{\nu_1} \left(\frac{V_{s_1}}{U_{s_1}}\right)^{\nu_2} \cdots \left(\frac{V_{s_{k_2}}}{U_{s_{k_2}}}\right)^{\nu_2},$$

the sum being over all $(t_1, t_2, \ldots, t_{k_1})$ and $(s_1, s_2, \ldots, s_{k_2})$ such that $t_i \neq s_j$, for all i and j, and $0 < t_1 < t_2 < \cdots < t_{k_1} < \rho$, $0 < s_1 < s_2 < \cdots < s_{k_2} < \rho$. The notation can be extended to more than two distinct ν exponents, but we won't need such sums in this paper.

Thus, for instance, the sums $\Sigma_{1,3}$, $\Sigma_{2,2}$, $\Sigma_{1,1,2}$ and $\Sigma_{1,1,1,1}$ are respectively

$$\sum_{s,\,t} \frac{V_s V_t^3}{U_s U_t^3}, \sum_{s<t} \frac{V_s^2 V_t^2}{U_s^2 U_t^2}, \sum_{\substack{r<s,\\ t\in(0,\rho)}} \frac{V_r V_s V_t^2}{U_r U_s U_t^2}, \sum_{q<r<s<t} \frac{V_q V_r V_s V_t}{U_q U_r U_s U_t},$$

where in each sum q, r, s and t are distinct integers in the interval $(0, \rho)$.

Lemma 19. *We have for all primes $p \geq 7$ of maximal ranks*

$$\Sigma_{1,1,1} \equiv 0 \pmod{p^2} \text{ and } \Sigma_{1,1,1,1} \equiv \begin{cases} 0 \pmod{p}, & \text{if } \epsilon_p = 0 \text{ or } -1; \\ D^2 \pmod{p}, & \text{if } \epsilon_p = 1. \end{cases}$$

Proof. We have the linear system

$$\begin{aligned} \Sigma_1^3 - \Sigma_3 &= 3\Sigma_{1,2} + 6\Sigma_{1,1,1}, \\ \Sigma_1 \cdot \Sigma_{1,1} &= \Sigma_{1,2} + 3\Sigma_{1,1,1}. \end{aligned}$$

Because p^2 divides both Σ_1 and Σ_3, $\Sigma_1^3 - \Sigma_3$ and $\Sigma_1 \cdot \Sigma_{1,1}$ are each $0 \pmod{p^2}$. Since the determinant of the system is prime to p, $\Sigma_{1,2}$ and $\Sigma_{1,1,1}$ are both $0 \pmod{p^2}$.

From Lemma 10 with $p > 5$, which yields the values of Σ_2 and $\Sigma_4 \pmod p$, we deduce that

$$\Sigma_{2,2} = \frac{1}{2}(\Sigma_2^2 - \Sigma_4) \equiv \begin{cases} 0 \pmod p, & \text{if } \epsilon_p = 0 \text{ or } -1; \\ 3D^2 \pmod p, & \text{if } \epsilon_p = 1. \end{cases}$$

Now $\Sigma_{1,3} = \Sigma_1 \cdot \Sigma_3 - \Sigma_4 \implies \Sigma_{1,3} \equiv -\Sigma_4 \pmod p$. Moreover, $2\Sigma_{1,1,2} + 2\Sigma_{2,2} + \Sigma_{1,3} = \Sigma_{1,2} \cdot \Sigma_1 \equiv 0 \pmod p$.

Thus, $\Sigma_{1,1,2}$ is $0 \pmod p$, if ϵ_p is 0 or -1, and $\Sigma_{1,1,2}$ is $-4D^2 \pmod p$, if ϵ_p is 1.

Therefore, as $6\Sigma_{1,1,1,1} = \Sigma_{1,1}^2 - \Sigma_{2,2} - 2\Sigma_{1,1,2}$, we obtain, using Lemma 11, the desired congruences for $\Sigma_{1,1,1,1}$. □

Our first theorem is a generalization of congruence (25).

Theorem 20. *Let (U, V) be a pair of Lucas sequence with parameters P and Q. Let p be a prime at least 7 of maximal rank ρ equal to $p - \epsilon_p$. Then*

$$\binom{2\rho-1}{\rho-1}_U \equiv \left(\frac{V_\rho}{2}\right)^{\rho-1}\left(1 + \frac{U_\rho}{V_\rho}\sum_{0<t<\rho}\frac{V_t}{U_t} + \frac{U_\rho^2}{V_\rho^2}\sum_{0<s<t<\rho}\frac{V_sV_t}{U_sU_t} + R\right) \pmod{p^5},$$

$$\textit{where } \; R = \frac{\epsilon_p(1+\epsilon_p)}{2}\frac{D^2U_\rho^4}{V_\rho^4} = \begin{cases} 0, & \textit{if } \epsilon_p = 0 \textit{ or } -1; \\ D^2U_\rho^4/V_\rho^4, & \textit{if } \epsilon_p = 1. \end{cases}$$

Proof. Expanding the product $2^{\rho-1}\prod_{t=1}^{\rho-1} U_{\rho+t} = \prod_{t=1}^{\rho-1}(V_\rho U_t + U_\rho V_t)$ as we did early in the proof of Theorem 3, but up to the fourth power of U_ρ, yields that $2^{\rho-1}\binom{2\rho-1}{\rho-1}_U$ is congruent to

$$V_\rho^{\rho-1} + V_\rho^{\rho-2}U_\rho\Sigma_1 + V_\rho^{\rho-3}U_\rho^2\Sigma_{1,1} + V_\rho^{\rho-4}U_\rho^3\Sigma_{1,1,1} + V_\rho^{\rho-5}U_\rho^4\Sigma_{1,1,1,1} \pmod{p^5}.$$

Applying the congruences obtained in Lemma 19 to the last two terms of the above sum yields the theorem. □

We now prove a congruence formula that generalizes (26), but also generalizes Theorem 3 when $k = 1$. The method of proof brings out the factor $(-1)^{\epsilon_p}Q^{\rho(\rho-1)/2}$ naturally, albeit in the equivalent form $(-1)^{\rho-1}Q^{\rho(\rho-1)/2}$. It is particularly appealing because it only contains two terms, no more than (26), and is valid regardless of the value of the maximal rank ρ.

Theorem 21. *Let (U, V) be a pair of Lucas sequence with parameters P and Q. Let p be a prime at least 7 of maximal rank ρ equal to $p - \epsilon_p$. Then*

$$\binom{2\rho-1}{\rho-1}_U \equiv (-1)^{\rho-1}Q^{\frac{\rho(\rho-1)}{2}}\left(1 + 2\frac{U_\rho}{V_\rho}\sum_{0<t<\rho}\frac{V_t}{U_t}\right) \pmod{p^5}.$$

Proof. All unmarked sums and products are for t running from 1 to $\rho-1$. Note that $\prod U_t = \prod U_{\rho-t}$. Thus by (18) we may write

$$\begin{aligned} 2^{\rho-1}Q^{\sum t}\prod U_t &= \prod 2Q^t U_{\rho-t} = \prod (U_\rho V_t - V_\rho U_t) \\ &= (-V_\rho)^{\rho-1}\prod\left(1-\frac{U_\rho}{V_\rho}\frac{V_t}{U_t}\right)\prod U_t. \end{aligned}$$

Therefore

$$(-1)^{\rho-1}Q^{\rho(\rho-1)/2} = \left(\frac{V_\rho}{2}\right)^{\rho-1}\prod\left(1-\frac{U_\rho}{V_\rho}\frac{V_t}{U_t}\right),$$

so that $(-1)^{\rho-1}Q^{\rho(\rho-1)/2}$ is congruent to

$$\left(\frac{V_\rho}{2}\right)^{\rho-1}\left(1-\frac{U_\rho}{V_\rho}\Sigma_1+\frac{U_\rho^2}{V_\rho^2}\Sigma_{1,1}-\frac{U_\rho^3}{V_\rho^3}\Sigma_{1,1,1}+\frac{U_\rho^4}{V_\rho^4}\Sigma_{1,1,1,1}\right) \pmod{p^5}. \tag{28}$$

Note that from (28) we recover the congruence

$$(-1)^{\rho-1}Q^{\rho(\rho-1)/2} \equiv \left(\frac{V_\rho}{2}\right)^{\rho-1} \pmod{p^2}. \tag{29}$$

Subtracting the expansion in (28) from that of $\binom{2\rho-1}{\rho-1}_U$ obtained in the proof of Theorem 20, we find that

$$\begin{aligned} \binom{2\rho-1}{\rho-1}_U - (-1)^{\rho-1}Q^{\rho(\rho-1)/2} &\equiv \left(\frac{V_\rho}{2}\right)^{\rho-1}\left(2\frac{U_\rho}{V_\rho}\Sigma_1+2\frac{U_\rho^3}{V_\rho^3}\Sigma_{1,1,1}\right) \\ &\equiv 2\left(\frac{V_\rho}{2}\right)^{\rho-1}\frac{U_\rho}{V_\rho}\Sigma_1 \pmod{p^5}, \end{aligned}$$

since $\Sigma_{1,1,1}$ is $0 \pmod{p^2}$ by Lemma 19. In the above congruence as $\frac{U_\rho}{V_\rho}\Sigma_1$ is $0 \pmod{p^3}$ we may, by (29), replace $\left(\frac{V_\rho}{2}\right)^{\rho-1}$ by $(-1)^{\rho-1}Q^{\rho(\rho-1)/2}$ and deduce our theorem. □

Lemma 22. *Suppose ν is a nonnegative integer. Let $p \geq \nu+5$ be a prime of maximal rank, say ρ. Then*

$$\sum_{0<t<\rho}\frac{4Q^t}{U_t^2}\frac{V_t^\nu}{U_t^\nu} = \Sigma_{\nu+2}-D\Sigma_\nu \equiv \begin{cases} 0 \pmod{p^2}, & \textit{if } \nu \textit{ is odd;} \\ 0 \pmod{p}, & \textit{if } \nu \textit{ is even.} \end{cases}$$

Proof. We have

$$\sum_{0<t<\rho}\frac{4Q^t}{U_t^2}\frac{V_t^\nu}{U_t^\nu} = \sum_{0<t<\rho}\frac{(V_t^2-DU_t^2)}{U_t^2}\frac{V_t^\nu}{U_t^\nu} = \Sigma_{\nu+2}-D\Sigma_\nu.$$

If ν is odd, then, $p \geq \nu+5$ implies, by Lemma 10, that both Σ_ν and $\Sigma_{\nu+2}$ are $0 \pmod{p^2}$. If ν is even, then both $\Sigma_{\nu+2}$ and $D\Sigma_\nu$ are $0 \pmod{p}$, when ρ is p or $p+1$, by Lemma 10. If ρ is $p-1$, then by the same lemma $\Sigma_{\nu+2}-D\Sigma_\nu \equiv -2D^{\frac{\nu+2}{2}} - D(-2D^{\nu/2}) \equiv 0 \pmod{p}$. □

Lemma 23. *We have for all primes $p \geq 7$ of maximal rank ρ*

$$-2\Sigma_1 \equiv \frac{U_\rho}{V_\rho} \sum_{0<t<\rho} \frac{4Q^t}{U_t^2} \pmod{p^4}.$$

Proof. All sums are over an index t running from 1 to $\rho - 1$.

$$\begin{aligned} -2\Sigma_1 &= -\sum \left(\frac{V_t}{U_t} + \frac{V_{\rho-t}}{U_{\rho-t}} \right) = -2U_\rho \sum \frac{1}{U_t U_{\rho-t}}, \text{ by (13)}, \\ &= -2U_\rho \sum \frac{2Q^t}{U_t(U_\rho V_t - U_t V_\rho)}, \text{ using (18)}, \\ &= 2\frac{U_\rho}{V_\rho} \sum \frac{2Q^t}{U_t^2(1 - \frac{V_t}{U_t}\frac{U_\rho}{V_\rho})} \\ &\equiv \frac{U_\rho}{V_\rho} \sum \frac{4Q^t}{U_t^2} \left(1 + \frac{V_t}{U_t}\frac{U_\rho}{V_\rho} + \frac{V_t^2}{U_t^2}\frac{U_\rho^2}{V_\rho^2} \right) \pmod{p^4}, \end{aligned}$$

yielding the lemma because, by Lemma 22, $U_\rho^{\nu+1} \sum \frac{4Q^t}{U_t^2} \frac{V_t^\nu}{U_t^\nu}$ is 0 (mod p^4), for $\nu = 1$ and $\nu = 2$, if $p \geq 7$. □

From Theorem 21, it is not difficult to reach a third theorem that generalizes (27).

Theorem 24. *Let (U, V) be a pair of Lucas sequence with parameters P and Q. Let p be a prime at least 7 of maximal rank ρ equal to $p - \epsilon_p$. Then*

$$\binom{2\rho - 1}{\rho - 1}_U \equiv (-1)^{\epsilon_p} Q^{\frac{\rho(\rho-1)}{2}} \left(1 - 4\frac{U_\rho^2}{V_\rho^2} \sum_{0<t<\rho} \frac{Q^t}{U_t^2} \right) \pmod{p^5}.$$

Proof. In the congruence for the Lucasnomial $\binom{2\rho-1}{\rho-1}_U$ of Theorem 21 we may replace $2\frac{U_\rho}{V_\rho}\Sigma_1$ by $-\frac{U_\rho^2}{V_\rho^2} \sum \frac{4Q^t}{U_t^2}$ since by Lemma 23 the two expressions are congruent modulo p^5. □

Remark 25. In stating Theorem 24 we chose the expression $-4\frac{U_\rho^2}{V_\rho^2} \sum \frac{Q^t}{U_t^2}$ rather than $-\frac{U_\rho^2}{V_\rho^2}\Sigma_2 + \frac{U_\rho^2}{V_\rho^2}(\rho - 1)D$ because it contains only one term; that term is 0 (mod p^3) and it reduces to $-p^2 \sum \frac{1}{t^2}$ for $U = U(2, 1)$.

Lemma 26. *We have for all primes $p \geq 7$ of maximal rank ρ*

$$\frac{U_\rho}{V_\rho}\Sigma_1 \equiv \frac{U_\rho^2}{V_\rho^2}\Sigma_{1,1} - \frac{1}{2}\frac{U_\rho^2}{V_\rho^2}(\rho - 1)D \pmod{p^5}.$$

Proof. By Lemma 23, we see that

$$\frac{U_\rho}{V_\rho}\Sigma_1 \equiv -\frac{1}{2}\frac{U_\rho^2}{V_\rho^2}\sum_{0<t<\rho}\frac{4Q^t}{U_t^2} \pmod{p^5}.$$

By Lemma 22,

$$\sum_{0<t<\rho}\frac{4Q^t}{U_t^2} = \Sigma_2 - D(\rho-1).$$

Thus, as $\Sigma_2 = \Sigma_1^2 - 2\Sigma_{1,1} \equiv -2\Sigma_{1,1} \pmod{p^4}$, the lemma follows. □

By using Lemma 26 and Theorem 21 we obtain another generalization of (25) slightly different from that given in Theorem 20, which we now state.

Theorem 27. *Let (U,V) be a pair of Lucas sequences with parameters P and Q. Let p be a prime at least 7 of maximal rank ρ equal to $p-\epsilon_p$. Then $\binom{2\rho-1}{\rho-1}_U$ is congruent to*

$$(-1)^{\epsilon_p}Q^{\frac{\rho(\rho-1)}{2}}\left(1+\frac{U_\rho}{V_\rho}\sum_{0<t<\rho}\frac{V_t}{U_t}+\frac{U_\rho^2}{V_\rho^2}\sum_{0<s<t<\rho}\frac{V_sV_t}{U_sU_t}-\frac{1}{2}D\frac{U_\rho^2}{V_\rho^2}(\rho-1)\right) \pmod{p^5}.$$

We end the paper with a congruence for $\binom{2\rho-1}{\rho-1}_U$ modulo p^6. It generalizes Theorem 2.4 of [33] which says that

$$\binom{2p-1}{p-1} \equiv 1+2p\sum_{0<t<p}\frac{1}{t}+\frac{2p^3}{3}\sum_{0<t<p}\frac{1}{t^3} \pmod{p^6},$$

for all primes $p \geq 7$, and also generalizes our Theorem 21.

Theorem 28. *Let (U,V) be a pair of Lucas sequences with parameters P and Q. Let p be a prime at least 7 of maximal rank ρ. Then*

$$\binom{2\rho-1}{\rho-1}_U \equiv (-1)^{\rho-1}Q^{\frac{\rho(\rho-1)}{2}}\left(1+2\frac{U_\rho}{V_\rho}\sum_{0<t<p}\frac{V_t}{U_t}+\frac{2}{3}\frac{U_\rho^3}{V_\rho^3}\sum_{0<t<p}\frac{V_t^3}{U_t^3}\right) \pmod{p^6}.$$

Proof. We proceed as in Lemma 19 to show that $\Sigma_{1,1,1,1,1} \equiv 0 \pmod{p}$ (in fact 0 modulo p^2). By Lemma 10, the expressions $\Sigma_1 \cdot \Sigma_4 - \Sigma_5$, $\Sigma_{1,1} \cdot \Sigma_3$, $\Sigma_1 \cdot \Sigma_{1,3}$ and $\Sigma_1 \cdot \Sigma_{2,2}$ are all 0 $\pmod{p^2}$, so we deduce, successively, that the sums $\Sigma_{1,4}$, $\Sigma_{1,1,3}$, $\Sigma_{2,3}$ and $\Sigma_{1,2,2}$ are each 0 $\pmod{p^2}$. Therefore, modulo p^2, we obtain the linear system

$$\begin{aligned}\Sigma_1 \cdot \Sigma_{1,1,1,1} &\equiv 5\,\Sigma_{1,1,1,1,1} + \Sigma_{1,1,1,2},\\ \Sigma_1^5 - \Sigma_5 &\equiv 120\,\Sigma_{1,1,1,1,1} + 60\,\Sigma_{1,1,1,2}.\end{aligned}$$

As its determinant, $2^2 \cdot 3^2 \cdot 5$, is prime to p, and its left members are each 0 $\pmod{p^2}$, we find that $\Sigma_{1,1,1,1,1} \equiv 0 \pmod{p^2}$.

Since $\Sigma_{1,1,1,1,1}$ is $0 \pmod{p}$, both the congruence for $\binom{2\rho-1}{\rho-1}_U$, derived from the proof of Theorem 20, and congruence (28) remain valid when we raise the modulus from p^5 to p^6. Hence,

$$\binom{2\rho-1}{\rho-1}_U - (-1)^{\rho-1}Q^{\rho(\rho-1)/2} \equiv \left(\frac{V_\rho}{2}\right)^{\rho-1}\left(2\frac{U_\rho}{V_\rho}\Sigma_1 + 2\frac{U_\rho^3}{V_\rho^3}\Sigma_{1,1,1}\right) \pmod{p^6}. \tag{30}$$

Suppose first that $\epsilon_p = -1$ or $\epsilon_p = 0$. Then, as $\Sigma_{1,1} \equiv 0 \pmod{p}$, we find that (29) is valid modulo p^3. Thus, we may replace $(V_\rho/2)^{\rho-1}$ in (30) by $(-1)^{\rho-1}Q^{\rho(\rho-1)/2}$ and obtain that

$$\binom{2\rho-1}{\rho-1}_U \equiv (-1)^{\rho-1}Q^{\rho(\rho-1)/2}\left(1 + 2\frac{U_\rho}{V_\rho}\Sigma_1 + 2\frac{U_\rho^3}{V_\rho^3}\Sigma_{1,1,1}\right) \pmod{p^6}. \tag{31}$$

Looking at the linear system at the start of the proof of Lemma 19 modulo p^3 we find the system of congruences

$$\begin{aligned} 3\Sigma_{1,2} + 6\Sigma_{1,1,1} &\equiv -\Sigma_3, \\ \Sigma_{1,2} + 3\Sigma_{1,1,1} &\equiv 0. \end{aligned}$$

Solving for $\Sigma_{1,1,1}$, we see that $\Sigma_{1,1,1} \equiv \frac{\Sigma_3}{3} \pmod{p^3}$, which inserted in congruence (31) yields the theorem.

Suppose now $\epsilon_p = 1$. By (28) and Lemma 11, congruence (29), when the modulus is increased to p^3, becomes

$$(-1)^{\rho-1}Q^{\rho(\rho-1)/2} \equiv (V_\rho/2)^{\rho-1}(1 + DU_\rho^2/V_\rho^2) \pmod{p^3}.$$

Thus we may replace $(V_\rho/2)^{\rho-1}$ in (30) by $(-1)^{\rho-1}Q^{\rho(\rho-1)/2}(1 - DU_\rho^2/V_\rho^2)$, multiply out the resulting expression and remove the term in $U_\rho^5\Sigma_{1,1,1}$ which is $0 \pmod{p^7}$ to find that

$$\binom{2\rho-1}{\rho-1}_U \equiv (-1)^{\rho-1}Q^{\rho(\rho-1)/2}\left(1 + 2\frac{U_\rho}{V_\rho}\Sigma_1 + 2\frac{U_\rho^3}{V_\rho^3}(\Sigma_{1,1,1} - D\Sigma_1)\right) \pmod{p^6}.$$

Because Σ_1 is $0 \pmod{p^2}$ and $\Sigma_{1,1} \equiv D \pmod{p}$, the linear system of Lemma 19 taken modulo p^3 is

$$\begin{aligned} 3\Sigma_{1,2} + 6\Sigma_{1,1,1} &\equiv -\Sigma_3, \\ \Sigma_{1,2} + 3\Sigma_{1,1,1} &\equiv D\Sigma_1. \end{aligned}$$

Solving for $\Sigma_{1,1,1}$ yields $\Sigma_{1,1,1} \equiv D\Sigma_1 + \Sigma_3/3$ and the theorem holds. □

5 Appendix on the integrality of Lucasnomials

Lucas, with a nearly complete justification, indirectly asserted the integrality of Lucasnomials in his memoir [22, p. 203] by stating that the product of n consecutive terms of a (nondegenerate) U sequence is divisible by the product $U_1 \dots U_n$. Various proofs have appeared, often with restrictions on the sequence U. In fact, they have been shown to be integral via a combinatorial argument [9]. But with convention (12) we want to prove their integrality in full generality.

Proposition 29. *Let $U = (U_n)$ be a Lucas sequence with parameters P and Q. With the adoption of convention (12) the Lucasnomial coefficients $\binom{m}{n}_U$ are rational integers for all nonnegative integers m and n.*

Proof. If all U_n, $n > 0$, are nonzero then the frequently used induction argument [15, 16, 18] based on the general Lucas identity $U_{n+1}U_{m-n} - QU_nU_{m-n-1} = U_m$ works fine. We repeat the argument here. The induction is on m. So one proves the integrality of the Lucasnomial $\binom{m}{n}_U$ for $m > n \geq 1$ by observing that

$$\begin{aligned} U_{n+1}\binom{m-1}{n}_U - QU_{m-n-1}\binom{m-1}{n-1}_U &= \\ \left(U_{n+1}\frac{U_{m-n}}{U_n} - QU_{m-n-1}\right) \cdot \binom{m-1}{n-1}_U &= \\ \frac{U_m}{U_n} \cdot \binom{m-1}{n-1}_U = \binom{m}{n}_U &\quad , \end{aligned}$$

completing the induction. If some term U_n, $n \geq 1$, is 0 then U is degenerate and, as we saw early in Section 2, $\rho(\infty) \in \{2, 3, 4, 6\}$, where $\rho(\infty)$ is the least positive integer t such that $U_t = 0$. Note that we may always assume $m \geq 2n$. Thus the Lucasnomial $\binom{m}{n}_U$ is the quotient of a product of n consecutive U terms of indices all larger than n divided by $U_nU_{n-1} \cdots U_1$. If $\rho(\infty) = 2$, i.e., $U_2 = P = 0$, then $U_{2k+1} = (-1)^kQ^k$ and $U_{2k} = 0$, $(k \geq 0)$. Then $\binom{m}{n}_U$ is up to sign a positive power of Q. If $\rho(\infty) = 3$, then, as $U_3 = P^2 - Q$, the first few terms of U are $0, 1, P, 0, -P^3, -P^4, 0, P^6, P^7, 0, \cdots$. So $|U_t| = P^{t-1}$ if $3 \nmid t$. If $\rho(\infty) = 4$, then, as $U_4 = P^3 - 2PQ$ and $P \neq 0$, $P^2 = 2Q$ and we see that $|U_t| = 2^{\lfloor t/2 \rfloor}(P')^{t-1}$ if $4 \nmid t$, where $P = 2P'$. Omitting the 0 terms when $4 \mid t$, powers of 2 and P' in U_t are nondecreasing functions of t. A similar result holds for $\rho(\infty)$ equal to 6 when $P^2 = 3Q$ and, omitting terms divisible by 6, powers of 3 and of P' in U_t are nondecreasing functions of t, where in this case $P = 3P'$. The integrality of the Lucasnomials follows readily. □

6 Acknowledgments

We thank an anonymous referee for his clear report and few formal suggestions.

References

[1] C. Babbage, Demonstration of a theorem relating to prime numbers, *Edinburgh Philosophical J.*, **1** (1819), 46–49.

[2] D. F. Bailey, Two p^3 variations of Lucas' theorem, *J. Number Theory*, **35** (1990), 208–215.

[3] C. Ballot, Divisibility of Fibonomials and Lucasnomials via a general Kummer rule, *Fibonacci Quarterly*, to appear.

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

[5] C. Ballot, On a congruence of Kimball and Webb involving Lucas sequences, *J. Integer Seq.*, **17** (2014), Article 14.1.3.

[6] C. Ballot, Lucas sequences with cyclotomic root field, *Dissertationes Math.*, **490** (2013), 92 pp.

[7] C. Ballot, A further generalization of a congruence of Wolstenholme, *J. Integer Seq.*, **15** (2012), Article 12.8.6.

[8] A. Benjamin and E. Reiland, Combinatorial proofs of Fibonomial identities, to appear in the *Proceedings of the 16th International Conf. on Fibonacci Numbers and their Applic.*, July 2014, Rochester, NY, 7 pp.

[9] A. Benjamin and S. Plott, A combinatorial approach to Fibonomial coefficients, *Fibonacci Quart.*, **46/47** (2008/09), 7–9.

[10] V. Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, 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.

[11] R. D. Fray, Congruence properties of ordinary and q-binomial coefficients. *Duke Math. J.*, **34**, (1967) 467–480.

[12] 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.

[13] 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.

[14] H. W. Gould, The bracket function and Fontené-Ward generalized binomial coefficients with application to Fibonomial coefficients, *Fibonacci Quart.*, **7** (1969) 23–40, 55.

[15] V. E. Hoggatt, Jr., Fibonacci numbers and generalized binomial coefficients, *Fibonacci Quart.*, **5** (1967) 383–400.

[16] J. M. Holte, Residues of generalized binomial coefficients modulo a prime, *Fibonacci Quart.*, **38** (2000) 227–238.

[17] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.

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

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

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

[21] D. Knuth and H. Wilf, The power of a prime that divides a generalized binomial coefficient, *J. Reine Angew. Math.* **396** (1989), 212–219.

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

[23] R. J. McIntosh, On the converse of Wolstenholme's theorem, *Acta Arith.*, **71** (1995), 381–389.

[24] R. Meštroviċ, Wolstenholme's theorem: Its generalizations and extensions in the last hundred and fifty years (1862–2012), preprint available at http://arxiv.org/abs/1111.3057v2.

[25] R. Meštroviċ, Congruences for Wolstenholme primes, preprint available at http://arxiv.org/abs/1108.4178.

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

[27] H. Pan, A generalization of Wolstenholme's harmonic series congruence, *Rocky Mountain J. Math.*, **38** (2008), 1263–1269.

[28] H. Roskam, A quadratic analogue of Artin's conjecture on primitive roots. *J. Number Theory* **81** (2000), 93–109.

[29] H. Roskam, Erratum: "A quadratic analogue of Artin's conjecture on primitive roots" [J. Number Theory 81 (2000), 93–109], *J. Number Theory* **85** (2000), 108.

[30] B. Sagan and C. Savage, Combinatorial interpretations of binomial coefficient analogues related to Lucas sequences, *Integers* **10** (2010) #A52.

[31] R. Stanley, *Enumerative Combinatorics*, Volume 1. Second edition. Cambridge Studies in Advanced Mathematics, **49**. Cambridge University Press, 2012.

[32] A. Straub, A q-analog of Ljunggren's binomial congruence, 23rd International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2011), pp. 897–902, *Discrete Math. Theor. Comput. Sci. Proc.*, 2011.

[33] R. Tauraso, More congruences for central binomial coefficients. *J. Number Theory*, **130** (2010), 2639–2649.

[34] M. Ward, Note on divisibility sequences. *Bull. Amer. Math. Soc.* **42** (1936), 843–845.

[35] D. L. Wells, Lucas' theorem for generalized binomial coefficients, Ph. D. thesis, Washington State University, 1992.

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

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

[38] J. Zhao, Bernoulli numbers, Wolstenholme's theorem, and p^5 variations of Lucas' theorem. *J. Number Theory*, **123** (2007), 18–26.

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

Received October 24 2014; revised versions received December 18 2014; February 25 2015; March 21 2015; March 26 2015. Published in *Journal of Integer Sequences*, May 19 2015.

Return to Journal of Integer Sequences home page.