On a Congruence of Kimball and Webb Involving Lucas Sequences

Christian Ballot
Département de Mathématiques et Mécanique
Université de Caen
F-14032 Caen Cedex
France
christian.ballot@unicaen.fr

Abstract

Given a pair (U_t) and (V_t) of Lucas sequences, an odd integer $\nu \geq 1$, and a prime $p \geq \nu + 4$ of maximal rank ρ_U, i.e., such that ρ_U is p or $p \pm 1$, we show that $\sum_{0 < t < \rho_U} (V_t/U_t)^\nu \equiv 0 \pmod{p^2}$. This extends a result of Kimball and Webb, who proved the case $\nu = 1$. Some further generalizations are also established.

1 Introduction

The main purpose of this note is to provide a common generalization to Theorems 1 and 2 below.

Theorem 1. *Let $\nu \geq 1$ be an odd integer. Suppose $p \geq \nu + 4$ is a prime number. Then*

$$H_{p-1}^\nu := \sum_{t=1}^{p-1} \frac{1}{t^\nu} \equiv 0 \pmod{p^2}.$$

Theorem 2. *Let $U(P,Q)$, $V(P,Q)$ be a pair of Lucas sequences, $p \geq 5$, $p \nmid Q$, a prime of rank ρ equal to $p - \epsilon_p$, where $\epsilon_p = 0$ or ± 1. Then*

$$\sum_{t=1}^{\rho-1} \frac{V_t}{U_t} \equiv 0 \pmod{p^2}.$$

Theorem 1 appears in the book of Hardy and Wright [3] as Theorem 131 and is one of many generalizations of the 1862 congruence of Wolstenholme [10] which states that

$$H_{p-1} := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}, \tag{1}$$

i.e., that the numerator of the rational number H_{p-1} is a multiple of p^2, whenever p is a prime number at least 5. Sums of the type $\sum_{t=1}^{m} 1/t^{\nu}$, where ν is odd and t is prime to m, were first studied by Leudesdorf [6]. Their values modulo m^2 have been the subject of many papers and these results were revisited in the paper [9]. Historically, Wolstenholme used the congruence (1) to prove that for all primes $p \geq 5$ we have

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

a fact known as Wolstenholme's congruence. The survey paper [7] mentions many generalizations of the congruence (2), but also contains generalizations of the related congruence (1), particularly in Sections 4 and 8.

Theorem 2, as may not readily appear, is yet another (surprising!) generalization of the congruence (1) of Wolstenholme. Contrary to other known generalizations, its discovery by Kimball and Webb [5], who initially proved it for the special pair of Lucas sequences $U(1, -1)$, $V(1, -1)$ in the paper [4], came much later, and more than 130 years after (1) had appeared. For $(P, Q) = (2, 1)$, we have $x^2 - Px + Q = (x - 1)^2$, $U_t = t$ and $V_t = 2$ for all integers $t \geq 0$ so that every prime p has rank p, and we see that the result of Kimball and Webb is indeed a generalization of the congruence of Wolstenholme.

Putting Theorems 1 and 2 next to each other and computing a few sums such as $\sum_{t=1}^{7} L_t^3/F_t^3 \pmod{49}$ or $\sum_{t=1}^{9} L_t^5/F_t^5 \pmod{121}$, where L_t and F_t are the t-th Lucas and the t-th Fibonacci numbers, and finding in both cases $0 \pmod{p^2}$ for $p = 7$ and $p = 11$, respectively, led to conjecturing (ô res mirabile!) that Theorem 3 holds.

Theorem 3. *Let $\nu \geq 1$ be an odd integer and $U(P, Q)$, $V(P, Q)$ be a pair of Lucas sequences. If $p \geq \nu + 4$, $p \nmid Q$, is a prime of maximal rank ρ, i.e., of rank $p - \epsilon_p$, where $\epsilon_p = 0$ or ± 1, then*

$$\sum_{t=1}^{\rho-1} \frac{V_t^{\nu}}{U_t^{\nu}} \equiv 0 \pmod{p^2}.$$

We briefly remark that Theorem 2 of Kimball and Webb has recently been generalized in several directions. One generalization is found in [8], another in Chapter 4 of [1], and again another in [2], where congruences involving sums of ratios V_t/U_t of Lucas sequences taken modulo m^2, where m may be composite, not necessarily prime, were considered.

Theorem 2 was stated in a mildly generalized form in both papers [1] and [2], in part because it led to the further generalizations found in these papers. In anticipation of yet further tentative generalizations we wish to prove a more general version of Theorem 3, namely

Theorem 4. *Let $\nu \geq 1$ be an odd integer. Let $U(P,Q)$ and $V(P,Q)$ be a pair of Lucas sequences and $p \nmid Q$ be a prime number of maximal rank ρ with respect to $U(P,Q)$. Assume further that $p - 1 \nmid \nu \pm 1$ if $\nu \geq 3$ and $p - 1 \nmid \nu + 1$ if $\nu = 1$. Then, for all integers k, we have that*

$$S := \sum_{t=k\rho+1}^{(k+1)\rho-1} \frac{V_t^\nu}{U_t^\nu} \equiv 0 \pmod{p^2}.$$

Note that if $p \geq \nu + 4$ then $p - 1 \nmid \nu \pm 1$ when $\nu \geq 3$ and $p - 1 \nmid \nu + 1$ when $\nu = 1$ so that Theorem 4 implies Theorem 3 by setting $k = 0$.

A secondary purpose of our note is to indicate how one can obtain further results that combine the approach taken in [2], i.e., congruences with composite moduli m of maximal ranks, with the general odd exponents $\nu \geq 1$ of the present paper. This is done in the third and final section.

Throughout this note we assume familiarity with Lucas sequences. The introduction of the paper [2] contains references to Lucas theory and useful remarks and definitions concerning ranks of primes and integers, and congruences of rational numbers modulo an integer m.

2   Proof of Theorem 4

We begin by a few lemmas and remarks.

Lemma 5. *Let $\nu \geq 1$ be an odd integer, p be a prime number and x and y be two rational integers whose sum is divisible by p. Then there is a rational integer c, which may depend on ν, such that*

$$x^\nu + y^\nu \equiv c(xy)^{(\nu-1)/2}(x+y) \pmod{p^2}. \tag{3}$$

Proof. Choosing $c = 1$ we see that (3) holds for $\nu = 1$. We proceed by strong induction on ν. So given $\nu \geq 3$ we assume that for each $i = 1, \ldots, (\nu - 1)/2$, we have

$$x^{\nu-2i} + y^{\nu-2i} \equiv c_i(xy)^{(\nu-2i-1)/2}(x+y) \pmod{p^2},$$

for some $c_i \in \mathbb{Z}$.

Expanding $(x + y)^\nu$ by Newton's formula and pairing terms in $x^k y^{\nu-k}$ with terms in $x^{\nu-k} y^k$, we find that

$$
\begin{aligned}
x^\nu + y^\nu &= (x+y)^\nu - \binom{\nu}{1}xy(x^{\nu-2} + y^{\nu-2}) - \binom{\nu}{2}x^2 y^2(x^{\nu-4} + y^{\nu-4}) \\
&\quad - \cdots - \binom{\nu}{(\nu-1)/2}(xy)^{(\nu-1)/2}(x+y).
\end{aligned}
$$

The term $(x+y)^\nu$ is divisible by p^2 and, by the inductive hypothesis, each term $(xy)^i(x^{\nu-2i} + y^{\nu-2i})$ is congruent to $c_i(xy)^{(\nu-1)/2}(x+y)$ modulo p^2 for some integer c_i. Hence, putting $c = -\sum c_i\binom{\nu}{i}$, $i = 1, \ldots, (\nu - 1)/2$, the lemma follows. $\square$

3

Lemma 6. *Let p be an odd prime and $e \geq 0$ be an integer such that $p - 1 \nmid e$ if $e \geq 1$. Then the sum $\sum_{t=1}^{p} t^e$ is divisible by p.*

Proof. If e is 0, then the result is trivial. Assume $e \geq 1$. If g is a primitive root modulo p, then $g^e \not\equiv 1 \pmod{p}$. But $\sum_{t=1}^{p} t^e \equiv \sum_{t=1}^{p}(gt)^e \pmod{p}$. Hence, p divides $(g^e - 1)\sum_{t=1}^{p} t^e$. $\square$

Given a pair U, V of Lucas sequences with parameters (P, Q) we denote the discriminant $P^2 - 4Q$ by D and recall a few relevant identities. For all integers s and t, we have

$$
\begin{align}
2U_{s+t} &= U_s V_t + U_t V_s, \tag{4}\\
4Q^t &= V_t^2 - DU_t^2, \tag{5}\\
2Q^t U_{s-t} &= U_s V_t - U_t V_s, \tag{6}\\
2Q^t V_{s-t} &= V_s V_t - DU_s U_t. \tag{7}
\end{align}
$$

We are ready for a proof of Theorem 4.

Proof. All unmarked sums are taken with indices running from $k\rho + 1$ to $(k+1)\rho - 1$. Also we put $r := (2k+1)\rho$. Then we see that

$$
S = \frac{1}{2}\sum\left(\frac{V_t^\nu}{U_t^\nu} + \frac{V_{r-t}^\nu}{U_{r-t}^\nu}\right) = \frac{1}{2}\sum \frac{V_t^\nu U_{r-t}^\nu + U_t^\nu V_{r-t}^\nu}{U_t^\nu U_{r-t}^\nu}.
$$

Put $x = V_t U_{r-t}$ and $y = U_t V_{r-t}$. Then, by equation (4), $x + y = 2U_r$, which is divisible by p. Thus, by Lemma 5, we have for some integer c

$$
V_t^\nu U_{r-t}^\nu + U_t^\nu V_{r-t}^\nu \equiv 2cU_r (V_t U_{r-t} U_t V_{r-t})^{(\nu-1)/2} \pmod{p^2}.
$$

Therefore, if $p^2 \mid cU_r$, then $S \equiv 0 \pmod{p^2}$. So we assume $p^2 \nmid cU_r$. Then $S \equiv 0 \pmod{p^2}$ if and only if p divides

$$
\sum \frac{(V_t U_{r-t} U_t V_{r-t})^{(\nu-1)/2}}{U_t^\nu U_{r-t}^\nu}. \tag{8}
$$

By the subtraction formulas (6) and (7), we find that

$$
\begin{align}
(2U_{r-t})^{(\nu-1)/2} &\equiv (-1)^{(\nu-1)/2} Q^{-(\nu-1)t/2} U_t^{(\nu-1)/2} V_r^{(\nu-1)/2} \pmod{p}, \text{ and}\\
(2V_{r-t})^{(\nu-1)/2} &\equiv Q^{-(\nu-1)t/2} V_t^{(\nu-1)/2} V_r^{(\nu-1)/2} \pmod{p}.
\end{align}
$$

Thus, there exist integers λ_1 and λ_2, prime to p and not dependent on t, such that modulo p the numerator of the t-th term in (8) is equal to $\lambda_1 Q^{-(\nu-1)t} U_t^{\nu-1} V_t^{\nu-1}$, while its denominator is equal to $\lambda_2 Q^{-\nu t} U_t^{2\nu}$ since $(2U_{r-t})^\nu \equiv -Q^{-\nu t} U_t^\nu V_r^\nu \pmod{p}$. Indeed, by (5), $p \nmid V_r$. Thus, p^2 divides S iff

$$
p \text{ divides } \sum \frac{Q^t V_t^{\nu-1}}{U_t^{\nu+1}}.
$$

4

By (5) we see that $4Q^t V_t^{\nu-1} = V_t^{\nu+1} - DU_t^2 V_t^{\nu-1}$. Hence, S is zero modulo p^2 iff p divides

$$\sum \frac{V_t^{\nu+1}}{U_t^{\nu+1}} - D \sum \frac{V_t^{\nu-1}}{U_t^{\nu-1}}. \tag{9}$$

Note that since p is an odd prime and $p \nmid Q$, if s and t are distinct integers that belong to the interval $(k\rho, (k+1)\rho)$, then V_s/U_s and V_t/U_t are distinct modulo p by (6). Also, if D is a quadratic residue modulo p, then V_t/U_t and $\pm\sqrt{D}$ are not congruent modulo p by (5).

If ρ is $p+1$, then, as t varies from $k(p+1)+1$ to $k(p+1)+p$, $V_t/U_t \pmod{p}$ runs through all of $\mathbb{Z}/p\mathbb{Z}$. Thus, by Lemma 6, as $\nu \not\equiv \pm 1 \pmod{p-1}$, we find that both sums appearing in (9) are divisible by p. The same divisibilities hold if ρ is p, since, then, only the residue 0 $\pmod{p}$ is absent from each of the two sums. If ρ is $p-1$, then, as t varies from $k\rho+1$ to $k\rho+p-2$, $V_t/U_t \pmod{p}$ runs through all of $\mathbb{Z}/p\mathbb{Z}$ but $\pm\sqrt{D} \pmod{p}$. Hence we deduce respectively that

$$\sum \left(\frac{V_t}{U_t}\right)^{\nu\pm1} + (\sqrt{D})^{\nu\pm1} + (-\sqrt{D})^{\nu\pm1} \equiv 0 \pmod{p}.$$

So we find that

$$\sum \frac{V_t^{\nu+1}}{U_t^{\nu+1}} - D \sum \frac{V_t^{\nu-1}}{U_t^{\nu-1}} \equiv (0 - 2D^{(\nu+1)/2}) - D(0 - 2D^{(\nu-1)/2}) \equiv 0 \pmod{p}.$$

$\square$

Remark 7. If $D = 0$, then the hypothesis $p - 1 \nmid \nu + 1$ suffices.

3   Two more theorems

Given a Lucas sequence $U(P, Q)$ and an integer m prime to Q we denote the rank of m in U by $\rho(m)$.

By the definition which was introduced and motivated in [2], we say that a composite integer $m \geq 1$ has maximal rank with respect to a Lucas sequence $U(P, Q)$ if every prime power dividing m has maximal rank and the ranks of any two such prime powers are relatively prime. A power p^a has maximal rank in $U(P, Q)$ iff p has maximal rank and the rank $\rho(p^a)$ is equal to $p^{a-1}\rho(p)$.

Here, unlike in the paper [2], we will not look for an exhaustive theorem dealing with sums of terms V_t^ν/U_t^ν modulo squares of integers of maximal rank, but the partial results we will state and sketch will be enough to see how one could obtain such congruences.

We start by an extension of Theorem 4 to prime powers. The case $\nu = 1$ is in fact a corollary of Theorem 12 of [2].

Theorem 8. *Let $\nu \geq 1$ be an odd integer and U, V be a pair of Lucas sequences with parameters P and Q. Suppose $p \nmid Q$ is a prime satisfying $p > (\nu+3)/2$, $p \neq \nu$ and $p \neq \nu+2$. Assume p^a has maximal rank for some integer $a \geq 1$. Then for all integers k we have*

$$S := \sum_{t \in I} \frac{V_t^\nu}{U_t^\nu} \equiv 0 \pmod{p^{2a}},$$

where I is the set of integers in $\big(k\rho(p^a), (k+1)\rho(p^a)\big) \setminus \rho(p)\mathbb{Z}$.

Proof. The proof is actually an extension of that of Theorem 4. It is easy to upgrade Lemma 5. Suppose $p^a \mid x+y$. Then for each odd integer $\nu \geq 1$ there is a rational integer c such that

$$x^\nu + y^\nu \equiv c(xy)^{(\nu-1)/2}(x+y) \pmod{p^{2a}}. \tag{10}$$

Note that the sum S contains $p^{a-1}\big(\rho(p)-1\big)$ terms. We now have $r = (2k+1)\rho(p^a)$. So $2cU_r$ is at least divisible by p^a. So we will be through if we can show that the sum corresponding to the sum in (8) is $0 \pmod{p^a}$. But that will be true if the expression in (9) is also $0 \pmod{p^a}$, where now both sums are taken over all integers t in I. At this point note that Lemma 6 can also be upgraded so that $\sum_{t=1}^{p^a} t^e \equiv 0 \pmod{p^a}$ provided, again, $p-1 \nmid e$. Indeed, if g is a primitive root modulo p^a, then it reduces to a primitive root modulo p, so $p \nmid g^e - 1$ if $p-1 \nmid e$ and this gives the lemma. Note that as t varies through I all V_t/U_t are distinct modulo p^a. If $\rho(p)$ is $p+1$, then since the cardinality of I is p^a we deduce that

$$\sum_{t \in I} \left(\frac{V_t}{U_t}\right)^{\nu \pm 1} \equiv \sum_{t \in \mathbb{Z}/p^a} t^{\nu \pm 1} \equiv 0 \pmod{p^a}.$$

If $\rho(p)$ is p then V_t is never $0 \pmod{p}$ and the terms $V_t/U_t \pmod{p^a}$ run through all invertible elements of $\mathbb{Z}/p^a\mathbb{Z}$ as t runs through I. Thus g being a primitive root modulo p^a and φ being Euler's totient function, we find that

$$\sum_{t \in I} \left(\frac{V_t}{U_t}\right)^{\nu \pm 1} \equiv \sum_{t=0}^{\varphi(p^a)-1} g^{(\nu \pm 1)t} = \frac{g^{(\nu \pm 1)\varphi(p^a)} - 1}{g^{\nu \pm 1} - 1} \equiv 0 \pmod{p^a},$$

since $g^{(\nu \pm 1)} - 1$ is not divisible by p. This argument is not valid if $\nu = 1$ and the exponent of g is $\nu - 1$. But in that case the result nevertheless holds because

$$D \sum_{t \in I} \left(\frac{U_t}{V_t}\right)^{\nu - 1} = D \cdot |I| \equiv 0 \pmod{p^a},$$

so the expression in (9) is $0 \pmod{p^a}$.

If $\rho(p)$ is $p-1$, then I contains $p^a - 2p^{a-1}$ elements. So $V_t/U_t \pmod{p^a}$ runs through all $\mathbb{Z}/p^a$ except $\pm\sqrt{D} + ip \pmod{p^a}$ for $i = 1, 2, \ldots, p^{a-1}$. Hence, $(V_t/U_t)^2 \pmod{p^a}$ hits

6

each nonzero quadratic residue in $\mathbb{Z}/p^a$ twice except all $D + ip$, for $i = 1, \ldots, p^{a-1}$, as t runs through I. Therefore,

$$\sum_{t \in I} \left(\frac{V_t}{U_t} \right)^{\nu+1} \equiv \sum_{i=1}^{p^a} (i^2)^{(\nu+1)/2} - 2 \sum_{j=1}^{p^{a-1}} (D + jp)^{(\nu+1)/2} \pmod{p^a}.$$

Now

$$\sum_{j=1}^{p^{a-1}} (D + jp)^{(\nu+1)/2} = \sum_{u=0}^{(\nu+1)/2} \binom{(\nu+1)/2}{u} D^{(\nu+1)/2-u} p^u \sum_{j=1}^{p^{a-1}} j^u.$$

As $p - 1 > (\nu+1)/2$, $p^{a-1} \mid \sum_{j=1}^{p^{a-1}} j^u$ and, unless $u = 0$, $p^a \mid p^u \sum_{j=1}^{p^{a-1}} j^u$. Hence, as $p \neq \nu + 2$, we have

$$\sum_{t \in I} \left(\frac{V_t}{U_t} \right)^{\nu+1} \equiv 0 - 2D^{(\nu+1)/2} p^{a-1} \pmod{p^a}.$$

Since a similar argument is valid for $\nu - 1$ instead of $\nu + 1$ we see that $\sum_{t \in I} \frac{V_t^{\nu+1}}{U_t^{\nu+1}} - D \sum_{t \in I} \frac{V_t^{\nu-1}}{U_t^{\nu-1}}$ is congruent to

$$(0 - 2p^{a-1} D^{(\nu+1)/2}) - D(0 - 2p^{a-1} D^{(\nu-1)/2}) = 0 \pmod{p^a}.$$

$\square$

Theorem 9. *Let $\nu \geq 1$ be an odd integer and U, V be a pair of Lucas sequences with parameters P and Q. Suppose m is a positive integer prime to Q of maximal rank. Assume further that each prime factor p of m satisfies $p > (\nu+3)/2$, $p \neq \nu$ and $p \neq \nu+2$. Then for all integers k we have*

$$S := \sum_{t \in I} \frac{V_t^\nu}{U_t^\nu} \equiv 0 \pmod{m^2},$$

where I is the set of integers in $\big(k\rho(m), (k+1)\rho(m)\big) \setminus \bigcup_{p \mid m} \rho(p)\mathbb{Z}$.

The proof we sketch is similar to, but simpler than that of Theorem 14 of the paper [2].

Proof. Assume for simplicity that $k = 0$. We proceed by induction on the number of distinct prime factors of m. If m is a prime power, then this is Theorem 8. Say $m = p^a n$, where $p \nmid n$ is prime and $n > 1$. It suffices to show that $S \equiv 0 \pmod{n^2}$. Note that since n has maximal rank the theorem will hold for n by the inductive hypothesis. Write S as $S^* - S^{**}$, where

$$S^* := \sum_{i=0}^{\rho(p^a)-1} \sum_{\substack{t=i\rho(n)+1 \\ \rho(q) \nmid t, \text{ if } q \mid n}}^{(i+1)\rho(n)-1} \left(\frac{V_t}{U_t} \right)^\nu,$$

and

$$S^{**} := \sum_{\substack{t=1 \\ \rho(q)\nmid t,\text{ if } q\mid n}}^{p^{a-1}\rho(n)} \left(\frac{V_{\rho(p)t}}{U_{\rho(p)t}}\right)^{\nu} = \sum_{i=0}^{p^{a-1}-1} U_{\rho(p)}^{-\nu} \sum_{\substack{t=i\rho(n)+1 \\ \rho(q)\nmid t,\text{ if } q\mid n}}^{(i+1)\rho(n)-1} \left(\frac{V'_t}{U'_t}\right)^{\nu},$$

where the sequences $U'_t = U_{\rho(p)t} \cdot U_{\rho(p)}^{-1}$ and $V'_t = V_{\rho(p)t}$ are the Lucas sequences associated with $(P', Q') = (V_{\rho(p)}, Q^{\rho(p)})$ and the letter q stands for a prime. Note that all inner sums in S^* are $0 \pmod{n^2}$ and that, as n has maximal rank with respect to U', the same is true, by our inductive hypothesis again, of the inner sums of S^{**}. $\qquad\square$

Example 10. Consider the Lucas sequences U and V with parameters $P = 1$ and $Q = -9$. Then $D = 37$, $\rho(7) = 6$ and $\rho(37) = 37$. Thus, $m = 259 = 7 \cdot 37$ has maximal rank. Hence, by Theorem 9, we have for $\nu = 1, 3$ or 9

$$\sum_t \left(\frac{V_t}{U_t}\right)^{\nu} \equiv 0 \pmod{7^2 \cdot 37^2},$$

where t runs over all integers between 1 and $222 = 6 \cdot 37$ except for multiples of 6 or 37.

4 Acknowledgments

References

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

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

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, London, 1960.

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

[5] W. Kimball and W. Webb, Some generalizations of Wolstenholme's theorem, in *Applications of Fibonacci Numbers* **8** (Rochester, NY, 1998), Kluwer Acad. Publ., 1999, 213–218.

[6] C. Leudesdorf, Some results in the elementary theory of numbers, *Proc. Lond. Math. Soc.*, **20** (1889), 199–212.

[7] R. Meštrović, 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.

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

[9] I. Sh. Slavutskii, Leudesdorf's theorem and Bernoulli numbers, *Arch. Math.(Brno)*, **35** (1999) 299–303.

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

Return to Journal of Integer Sequences home page.