Journal of Integer Sequences, Vol. 17 (2014),
Article 14.8.8

Congruences Involving Sums of Ratios of Lucas Sequences

Evis Ieronymou
Department of Mathematics and Statistics
University of Cyprus
1687 Nicosia
Cyprus
ieronymou.evis@ucy.ac.cy

Abstract

Given a pair (U_t) and (V_t) of Lucas sequences, we establish various congruences involving sums of ratios $\frac{V_t}{U_t}$. More precisely, let p be a prime divisor of the positive integer m. We establish congruences, modulo powers of p, for the sum $\sum \frac{V_t}{U_t}$, where t runs from 1 to $r(m)$, the rank of m, and $r(q) \nmid t$ for all prime factors q of m.

1 Introduction

Wolstenholme's classic congruence dating back to 1862 is the following:

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

where $p \geq 5$ is a prime number. Kimball and Webb [4] found a generalization of the above congruence using Lucas sequences. In order to state it we need to recall some basic definitions and terminology: The pair of Lucas sequences (U_t) and (V_t) associated with a pair of coprime integers P and Q is given by the second-order linear recurrence

$$X_{n+2} = PX_{n+1} - QX_n,$$

and initial conditions $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$. We set $D = P^2 - 4Q$. Given an integer m let $r(m)$ denote, if it exists, the least positive integer such that m divides $U_{r(m)}$

and call it the rank of appearance (or apparition) of m. For a prime p with $\gcd(p, 2Q) = 1$ we know that $r(p)$ divides $p - \left(\frac{D}{p}\right)$, where $\left(\frac{D}{p}\right)$ is the Legendre symbol. A prime is called of maximal rank if $r(p) = p - \left(\frac{D}{p}\right)$.

Kimball and Webb's congruence is the following:

$$v_p\left(\sum_{t=1}^{r(p)-1} \frac{V_t}{U_t}\right) \geq 2,$$

when $p \geq 5$ is a prime of maximal rank. In the above inequality and in the rest of this note $v_p(x)$ denotes the standard p-adic valuation of the rational number x, where p is a prime number. Note that for $P = 2,\ Q = 1$ we recover Wolstenholme's congruence.

In turn, Ballot [2] generalized Kimball and Webb's congruence in the following:

Proposition 1. *Let (U_t) and (V_t) be a pair of Lucas sequences. If m is of maximal rank and* $\gcd(m, 6Q)$*=1 then*

$$v_q\left(\sum_{t \in I_m} \frac{V_t}{U_t}\right) \geq 2v_q(m),$$

where q is a prime divisor of m and

$$I_m = \{n : 1 \leq n \leq r(m)\} - \bigcup_{\substack{p \text{ is prime} \\ p \mid m}} \mathbb{Z} \cdot r(p).$$

Remark 2. Ballot [2] proves more, most notably the condition that $\gcd(m, 6) = 1$ is not there and a complete list of what happens in those cases is given. The reason we will assume that $\gcd(m, 6) = 1$ in this note will be explained later in the introduction.

The notion of maximal rank for composite m was introduced in [2] and is the following: We say that m has maximal rank if for any two prime divisors p, q of m with $a = v_p(m)$ and $b = v_q(m)$ we have that (i) p is of maximal rank, (ii) $r(p^a) = p^{a-1}r(p)$ and (iii) $\gcd(r(p^a), r(q^b)) = 1$ for $p \neq q$.

This notion has the obvious nuisance that it excludes many m. For example, if m is of maximal rank then it can have at most one prime divisor outside the prime divisors of $2D$ and moreover all its prime divisors must themselves be of maximal rank. A natural thing to ask is whether we can say anything definite with a weaker notion. The aim of this note is to clarify the situation.

Our first main result tells us what happens for prime powers.

Theorem 3. *Let (U_t) and (V_t) be a pair of Lucas sequences and let p be a prime with* $\gcd(p, 6Q) = 1$ *and $v_p(U_{r(p)}) = 1$.*

If p has maximal rank then

$$v_p\left(\sum_{t\in I_{p^a}}\frac{V_t}{U_t}\right)\geq 2a.$$

If p does not have maximal rank then

$$v_p\left(\sum_{t\in I_{p^a}}\frac{V_t}{U_t}\right)=2a-1.$$

The new thing in the above theorem is the inclusion of the case when p does not have maximal rank. It is crucial in the consideration of integers with more than one prime divisor.

Example 4. We consider the Fibonacci and Lucas numbers, i.e., the pair of Lucas sequences associated to $P=1$ and $Q=-1$.

• For $m=13^3$ we have $r(13)=7$ and so

$$S\equiv 0 \pmod{13^5},\quad S\not\equiv 0 \pmod{13^6},$$

where

$$S=\sum_{\substack{t=1\\ \gcd(t,7)=1}}^{7\cdot 13^2}\frac{L_t}{F_t}.$$

The second main result is concerned with integers with more than one prime divisor.

Theorem 5. *Let $m=p^a\prod_{i=1}^{\tau}q_i^{a_i}$ be the prime factorization of m. Suppose that $\gcd(p,6Q)$=1 and $v_p(U_{r(p)})=1$. Let $r=r(p)$ and $r_i=r(q_i)$.*

1. *We have that*

$$v_p\left(\sum_{t\in I_m}\frac{V_t}{U_t}\right)\geq \max(a,\mu+\epsilon),$$

where $\mu=\max\{v_p(r_i)\}$ and $\epsilon=\left(\frac{D}{p}\right)^2$.

2. *Suppose that either $\max\{v_p(r_i): r\nmid r_i\}=0$ or $\{r_i : r\nmid r_i\}=\emptyset$. Then*

$$v_p\left(\sum_{t\in I_m}\frac{V_t}{U_t}\right)\geq 2a-1.$$

If moreover p has maximal rank and $\gcd(r,r_i)=1$ for all r_i with $r\nmid r_i$ the above inequality is strict.

Note that we recover Ballot's result stated at the beginning as a special case. Below we give examples not covered by that.

Example 6. We continue with the Fibonacci and Lucas numbers. In each case $S = \sum_{I_m} \frac{L_t}{F_t}$.

- For $m = 7^4 \cdot 11^3$ we have $r(7) = 8$, $r(11) = 10$ and so
$$S \equiv 0 \pmod{7^7 \cdot 11^5}.$$
- For $m = 7 \cdot 17^2$ we have $r(7) = 8$, $r(17) = 9$ and so
$$S \equiv 0 \pmod{7^2 \cdot 17^3}.$$
- For $m = 7 \cdot 97$ we have $r(7) = 8$, $r(97) = 7^2$ and so
$$S \equiv 0 \pmod{7^3 \cdot 97}.$$
- For $m = 5 \cdot 11^2$ we have $r(5) = 5$, $r(11) = 10$ and so
$$S \equiv 0 \pmod{5^2 \cdot 11^3}.$$
- For $m = 79 \cdot 859^2$ we have $r(79) = r(859) = 78$ and so
$$S \equiv 0 \pmod{79^2 \cdot 859^3}.$$
- For $m = 37 \cdot 73$ we have $r(37) = 19$, $r(73) = 37$ and so
$$S \equiv 0 \pmod{37^2 \cdot 73}.$$
- For $m = 19 \cdot 73^2 \cdot 89^3 \cdot 97^4$ we have $r(19) = 18$, $r(73) = 37$, $r(89) = 11$, $r(97) = 49$ and so
$$S \equiv 0 \pmod{19^2 \cdot 73^3 \cdot 89^5 \cdot 97^7}.$$

Remark 7. Note that there is no claim for optimality in the congruences. It can be checked that when $m \in \{7 \cdot 17^2, 5 \cdot 11^2, 79 \cdot 859^2, 37 \cdot 73\}$ the congruences above are indeed optimal for each prime dividing m. However when $m = 7 \cdot 97$ the congruence is optimal modulo 97 but not modulo 7 as we actually have that $v_7(S) = 4$.

A few words about our assumptions and definitions. If we seek a nice generalization of Kimball and Webb's result summing up to $r(m)$ is more or less forced (cf. [2, pg. 7]). Now, if we want to say something about the sum modulo powers of prime divisors of m we want the individual terms to make sense modulo p for any prime p dividing m. That is why we exclude the multiples of $r(p)$ in the definition of I_m. This, however, has hidden ramifications since integers we excluded because of q might alter the sum modulo powers of p in an unpredictable way and we have to keep track of the various interactions as we add more primes.

In this note we only impose the condition that $v_p(U_{r(p)}) = 1$ and see what happens. This is a reasonable condition: from considering prime powers we see that I_m does not see the difference between p and $p^{v_p(U_{r(p)})}$. Moreover, when $v_p(U_{r(p)}) > 1$ we can still use Lemma 10 to draw conclusions. With regards to our other assumptions, the exclusion of 3 is mostly a matter of aesthetics: the same arguments would go through but we would have to subtract 1 in various results when working modulo powers of 3 thus complicating the statement of the results. The exclusion of 2 is qualitatively different: not only the results would be more tedious to write but they would require different arguments to establish. Finally, we take $\gcd(p, Q) = 1$ since otherwise $r(p)$ does not exist.

This note is organized as follows. In Section 2 we recall some basic facts about Lucas sequences and set up two auxiliary lemmata. In Section 3 we take care of the case when m is a prime power by proving our first main result. In Section 4 we move on to the case when m has more than one prime divisor, and we prove our second main result.

The assertions about the ranks of appearance in the examples were checked using the computer algebra system `magma`.

2 Preliminaries

Lucas sequences are well-studied and satisfy many identities. For the convenience of the reader we collect some well-known properties of Lucas sequences we will be using in the following lemma. The interested reader can look at [1], [5] or [6] and references therein for details of the proofs and much more about Lucas sequences. We remind the reader of our assumption that $\gcd(P, Q) = 1$.

Lemma 8. *1. If s, t are positive integers and s divides t then U_s divides U_t.*

2. m divides U_n if and only if $r(m)$ divides n.

3.

$$r(\operatorname{lcm}(a, b)) = \operatorname{lcm}(r(a), r(b)).$$

4. If $\gcd(n, 2Q) = 1$ and $r(n)$ does not divide either s or t then

$$\frac{V_s}{U_s} \equiv \frac{V_t}{U_t} \pmod{n} \Leftrightarrow s \equiv t \pmod{r(n)}.$$

5. (Law of repetition) If p is an odd prime and p divides U_n then

$$v_p(U_{kn}) = v_p(U_n) + v_p(k).$$

6. If $\ell = v_p(U_{r(p)})$ then $r(p^a) = p^{\max(a,\ell)-\ell} r(p)$.

Remark 9. For the sake of clarity, in order to make sense of the last two statements of the lemma when some $U_n = 0$ we use the conventions that $v_p(0) = \infty$ and $\infty - \infty = 0$. This has no relevance to the next two sections.

We now establish two auxiliary lemmata which we will be using in the next sections.

Lemma 10. *Let p be an odd prime, $s = r(p^a)$ and $\nu = v_p(U_s)$. Let $J \subset \mathbb{Z}$ be a finite set such that*

(i) none of its elements is divisible by $r(p)$, and

(ii) there is a k such that sending x to $ks - x$ maps J to J.

Let $\ell = v_p(U_{ks})$ and denote $ks - x$ by $\hat{x}$.

Then

$$v_p\left(\sum_{t\in J} \frac{V_t}{U_t}\right) = \ell + v_p\left(\sum_{t\in J} \frac{1}{U_t U_{\hat{t}}}\right),$$

$$2V_{ks} \sum_{t\in J} \frac{1}{U_t U_{\hat{t}}} \equiv D|J| - \sum_{t\in J} \left(\frac{V_t}{U_t}\right)^2 \pmod{p^{2\ell}}.$$

Moreover, if J' is the translation of J by s, i.e., $J' = J + s$, then J' satisfies the two assumptions (with the new k being $k+2$) and the value of $\sum \frac{1}{U_t U_{\hat{t}}}$ is multiplied by $\frac{4}{V_s^2} \pmod{p^\nu}$.

Proof. The easy algebraic manipulations (which are based on well known-formulae for Lucas sequences) that establish the result can be found in [2] or [4]. For completeness and the convenience of the reader, we repeat the main points here. The first equality can be easily established by using the equality

$$\frac{V_t}{U_t} + \frac{V_{\hat{t}}}{U_{\hat{t}}} = 2\frac{U_{ks}}{U_t U_{\hat{t}}}.$$

The congruence is established by noting that its left hand side equals

$$\sum_{t\in J} \frac{V_t V_{\hat{t}}}{U_t U_{\hat{t}}} + D|J|,$$

and that we also have

$$\sum_{t\in J} \frac{V_t V_{\hat{t}}}{U_t U_{\hat{t}}} = \frac{1}{2}\sum_{t\in J} \frac{(2U_{ks})^2}{(U_t U_{\hat{t}})^2} - \sum_{t\in J} \left(\frac{V_t}{U_t}\right)^2.$$

The only non-trivial part of the last sentence is the final assertion, which follows immediately from the fact that

$$2U_{s+t} \equiv U_t V_s \pmod{U_s}.$$

$\square$

Lemma 11. *Let $p \geq 5$ be a prime and $r = r(p)$.*

If p has maximal rank then

$$\sum_{t=1}^{r-1} \left(\frac{V_t}{U_t}\right)^2 \equiv D(r-1) \pmod{p}.$$

If p does not have maximal rank then

$$\sum_{t=1}^{r-1} \left(\frac{V_t}{U_t}\right)^2 \not\equiv D(r-1) \pmod{p}.$$

Proof. In the first case it is easy to calculate explicitly the set $\{\frac{V_t}{U_t} : 1 \leq t \leq r-1\}$ modulo p and establish the result (cf. [4, proof of Theorem]). For the second case, the result is established by hand for the cases $r = 2, 3, 4$. When $r \geq 5$ we will use [3, Theorem 1.1] which states that if $n \geq 5$ then

$$\sum_{t=1}^{n-1} \frac{V_t}{U_t} \equiv \frac{(n^2-1)D}{6} \cdot \frac{U_n}{V_n} \pmod{w_n^2},$$

where w_n is the largest divisor of U_n relatively prime to $U_1, \ldots, U_{n-1}$. Taking $n = r$ in the above, and noting that from our assumptions $\frac{(r^2-1)D}{6V_r}$ is not divisible by p we deduce that

$$v_p\left(\sum_{t=1}^{r-1} \frac{V_t}{U_t}\right) = v_p(U_r).$$

The result now follows from the two displayed formulas of Lemma 10 (taking $s = r$, $k = 1$ and $J = \{1, \ldots, r-1\}$). $\square$

3 The case of prime powers

In this section p is a prime with $\gcd(p, 6Q) = 1$ and $v_p(U_{r(p)}) = 1$.

Note that the second assumption implies that

$$r(p^a) = p^{a-1} r(p)\,,\ v_p(U_{r(p^a)}) = a.$$

Recall the definition

$$I_m = \{x : 1 \leq x \leq r(m)\} - \bigcup_{\substack{q \text{ is prime} \\ q \,|\, m}} \mathbb{Z} \cdot r(q).$$

Lemma 12. *Let $r = r(p)$. Then*

$$v_p\left(\sum_{t\in I_{p^a}}\left(\frac{V_t}{U_t}\right)^2 - D|I_{p^a}|\right) \quad \textit{is} \quad \begin{cases}\geq a, & \textit{if } p \textit{ has maximal rank;}\\ = a-1, & \textit{if not.}\end{cases}$$

Proof. Let $K := \ker(\mathbb{Z}/p^a \to \mathbb{Z}/p)$. Note that the elements of $\{\frac{V_t}{U_t} : t \in I_p\}$ are pairwise distinct modulo p, the elements of $\{\frac{V_t}{U_t} : t \in I_{p^a}\}$ are pairwise distinct modulo p^a, $\frac{V_t}{U_t} \equiv \frac{V_{t+r}}{U_{t+r}}$ (mod p) and $|I_{p^a}| = p^{a-1}|I_p|$. Hence, working in $\mathbb{Z}/p^a$ the set $\{\frac{V_t}{U_t} : t \in I_{p^a}\}$ is the disjoint union of the cosets $K + \frac{V_t}{U_t}$ with $t \in I_p$. Since $\sum_{x\in K} x = \sum_{x\in K} x^2 = 0 \in \mathbb{Z}/p^a$, we therefore have that

$$\sum_{t\in I_{p^a}}\left(\frac{V_t}{U_t}\right)^2 \equiv p^{a-1}\sum_{t\in I_p}\left(\frac{V_t}{U_t}\right)^2 \pmod{p^a}.$$

The result now follows from Lemma 11. ∎

Remark 13. It is clear that the same result holds if we replace I_{p^a} by $I_{p^a} + l\cdot r(p^a)$, where l is a positive integer.

Proof of Theorem 3: Combine Lemma 10 and Lemma 12. ∎

Remark 14. Looking at Lemma 10 and Lemma 12 it is easy to see what happens if we replace I_{p^a} by $I_{p^a} + l\cdot r(p^a)$ in Theorem 3: If p has maximal rank the result remains the same. If p does not have maximal rank then the result is the same when p does not divide $2l+1$ whereas the p-adic valuation is increased by at least one when p divides $2l+1$.

4 More than one prime divisor

In this section p is a prime with $\gcd(p, 6Q) = 1$ and $v_p(U_{r(p)}) = 1$.

First we recall the following well-known fact, easily established by Binet's formulae: Let U', V' denote the pair of Lucas sequences associated with $P' = V_n$, $Q' = Q^n$. Then

$$U_{nk} = U_n U'_k \text{ and } V_{nk} = V'_k. \tag{1}$$

It is also straightforward to see that: (i) If $r(p)$ divides n then $r'(p) = p$ and $v_p(U'_p) = 1$, (ii) If $r(p)$ does not divide n then $r'(p) = \frac{r(p)}{d}$ and $v_p(U'_{r'(p)}) = v_p(U_{r(p)}) + v_p(\frac{n}{d})$ where $d = \gcd(r(p), n)$.

Next, we fix some notation. For a finite set $J \subset \mathbb{Z}$ denote

$$S(J) := \sum_{t\in J}\frac{V_t}{U_t}.$$

Trivially

$$S(X\cup Y) = S(X) + S(Y) - S(X\cap Y),$$

and so if three of the above terms have p-adic valuation at least ν then so does the fourth. We will use this with no further mention.

Recall that if X is a subset of $\mathbb{Z}$ we write

$$X + n = \{x + n : x \in X\} \quad \text{and} \quad n \cdot X = \{nx : x \in X\}.$$

We also introduce the following:

$$L_{n:b_1,..,b_k} := \{x : 1 \le x \le n\} - \bigcup_{1 \le i \le k} \mathbb{Z} \cdot b_i.$$

Whenever we use the notation above, we will always have that n is divisible by all the b_i's.

We list some identities which are elementary to establish

$$L_{nsb:b} = \bigsqcup_{0 \le t \le n-1} L_{sb:b} + tsb, \tag{2}$$

$$L_{n:b_1,\ldots,b_k} \cap L_{n:b_{k+1},\ldots,b_{k+t}} = L_{n:b_1,\ldots,b_{k+t}}, \tag{3}$$

$$L_{n:b_1,\ldots,b_k,c_1} \cup L_{n:b_1,\ldots,b_k,c_2} = L_{n:b_1,\ldots,b_k,\mathrm{lcm}(c_1,c_2)}, \tag{4}$$

$$L_{n:b,c} \cup (L_{n:b} \cap L^*_{n:c}) = L_{n:b}, \tag{5}$$

$$L_{n:b} \cap L^*_{n:c} = c \cdot L_{\frac{n}{c}:\frac{b}{\gcd(b,c)}}, \tag{6}$$

where "$\bigsqcup$" stands for disjoint union and $L^*_{n:c}$ is the complement of $L_{n:c}$ in $L_{n:n}$.

We are now ready to prove our main result.

Proof of Theorem 5: Let

$$N = v_p\left(\sum_{t \in I_m} \frac{V_t}{U_t}\right) = v_p(S(I_m)).$$

1. By Lemma 10 we have that $N \ge v_p(U_{r(m)}) = a + v_p\left(\frac{r(m)}{r(p^a)}\right)$. Since

$$r(m) = \mathrm{lcm}(p^{a-1}r, r(q_i^{a_i})), \tag{7}$$

   the result then follows from the fact that $v_p(r) = 1$ when p divides D and $v_p(r) = 0$ when p does not divide D.

2. By Theorem 3, Remark 14 and formula (2) we have that

$$v_p(S(L_{nr:r})) \geq 2v_p(n) + 1. \tag{8}$$

Write $\{1 \leq i \leq \tau\} = T \bigsqcup T'$ where $i \in T'$ if and only if r divides r_i. Note that if $T = \emptyset$ then $I_m = L_{r(m):r,r_1,\ldots,r_\tau} = L_{r(m):r}$, and we are done by what was said above. To treat the case when $T \neq \emptyset$ we first establish the following.

Claim: Let c be the lcm of some of the r_i with $i \in T$. Then

$$v_p(S(L_{r(m):r,c})) \geq 2a - 1.$$

Proof of claim: By equation (5) it suffices to show that

$$v_p(S(L_{r(m):r})) \geq 2a - 1 \quad \text{ and } \quad v_p(S(L_{r(m):r} \cap L^*_{r(m):c}) \geq 2a - 1.$$

Using (8) and (7) we immediately get the first inequality. If r divides c then $L_{r(m):r}$ equals $L_{r(m):r,c}$ and we are done. Hence, we may assume that r does not divide c.

By (6) and (1) we have that

$$S(L_{r(m):r} \cap L^*_{r(m):c}) = \frac{1}{U_c} \sum_{t \in M} \frac{V'_t}{U'_t}, \quad \text{where} \quad M = L_{\frac{r(m)}{c}:\frac{r}{\gcd(r,c)}}$$

and U', V' are defined as in the beginning of this section with $n = c$. Since $v_p(r_i) = 0$ when $i \in T$, we have that $v_p(c) = 0$. Hence, our assumptions imply that $v_p(U'_{r'(p)}) = 1$ and $r'(p) = \frac{r}{\gcd(r,c)}$. Therefore, we deduce by (8) that $v_p(S(L_{r(m):r} \cap L^*_{r(m):c}) \geq 2\gamma + 1$, where $\gamma = v_p\left(\frac{r(m)}{\operatorname{lcm}(r,c)}\right)$. Since

$$v_p\left(\frac{r(m)}{\operatorname{lcm}(r,c)}\right) = v_p\left(\frac{r(m)}{r}\right) \geq a - 1,$$

the proof of the claim is complete. QED

It is now an easy induction using (3) and (4) to augment the claim to

$$v_p(S(L_{r(m):r,c,r_{i_1},\ldots,r_{i_k}})) \geq 2a - 1,$$

where $i_j \in T$.

Note that if p has maximal rank and $\gcd(r, r_i) = 1$ for all $i \in T$ then whenever we invoke Theorem 3 in the proof above the corresponding inequality is strict, and so in this case the result is that $v_p(S(L_{r(m):r,c,r_{i_1},\ldots,r_{i_k}})) > 2a - 1$.

Finally, to finish the proof we need only note that by definition $I_m = L_{r(m):r,r_1,\ldots,r_\tau}$, and that this set is unaltered if we omit all the r_i's that are multiples of r. □

Remark 15. Looking at the proof, it is not difficult to see that the same results hold if we replace I_m by $I_m + l \cdot r(m)$, where l is a positive integer.

References

[1] C. Ballot, Density of prime divisors of linear recurrences. *Mem. Amer. Math. Soc.* **115** (1995), no. 551.

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

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

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

[5] P. Ribenboim, *The Book of Prime Number Records*. Second edition. Springer-Verlag, 1989.

[6] E. Roettger, A cubic extension of the Lucas functions. Ph. D. thesis, University of Calgary, Canada, 2009.

2010 *Mathematics Subject Classification*: Primary 11B39; Secondary 11A07.
Keywords: Lucas sequence, rank of appearance, congruence.

Received June 5 2014; revised versions received July 18 2014; August 1 2014; August 8 2014. Published in *Journal of Integer Sequences*, August 12 2014.

Return to Journal of Integer Sequences home page.