Journal of Integer Sequences, Vol. 15 (2012),
Article 12.8.6

A Further Generalization of a Congruence of Wolstenholme

Christian Ballot
L.M.N.O., CNRS UMR 6139
Université de Caen
F-14032 Caen Cedex
France
christian.ballot@unicaen.fr

Abstract

Given a pair (U_t) and (V_t) of Lucas sequences, Kimball and Webb showed that $\sum_{0<t<\rho_U} \frac{V_t}{U_t} \equiv 0 \pmod{p^2}$, if p is a prime ≥ 5 whose rank ρ_U is maximal, that is to say, ρ_U is p or $p \pm 1$. We extend their result replacing p by a composite integer m of maximal rank, thereby providing a generalization of a classical congruence of Leudesdorf.

1 Introduction

In an 1862 paper of Wolstenholme [16], we find the congruence

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

i.e., the numerator of the rational number H_{p-1} is a multiple of p^2, whenever p is a prime number at least 5. Many elementary generalizations of this congruence were subsequently discovered, some before, some after 1900. Chapter VIII of the book [4] provides an attractive selection of some of the results that extend the congruence of Wolstenholme. Leudesdorf [9], in 1889, studied the sums $\sum_{t=1}^{m} 1/t^{\nu}$, where m is a positive integer, ν is an odd positive integer, and t runs over all integers from 1 to m that are prime to m. The simplest and most striking case, as Chowla refers to it, of the results of Leudesdorf is that of $\nu = 1$ and m prime to 6, for which we have that the sum $\sum_{t=1}^{m} 1/t$, t prime to m, is congruent to $0 \pmod{m^2}$, a clear generalization of the Wolstenholme congruence. Chowla [3] actually gave a concise half-page natural proof of this case. The theorem of Leudesdorf we will refer to in this paper is Theorem 128 of [4]. It corresponds to the case $\nu = 1$ without the restriction that m be prime to 6. Hardy and Wright refer to it as a comprehensive generalization of Wolstenholme's congruence. Thus, it predicts Wolstenholme's congruences for H_{p-1} not just for primes prime to 6, i.e., primes ≥ 5, but also for p equal to 2 and 3. We state this Leudesdorf theorem below.

Theorem 1. *Let m be an integer ≥ 1. Then*

$$\sum_{\substack{t=1\\ \gcd(t,m)=1}}^{m} \frac{1}{t} \quad \textit{is congruent to } 0 \pmod{m^2/e_m},$$

where

$$e_m = \begin{cases} 4, & \textit{if } m = 2^a,\ a \geq 1; \\ \gcd(m,6), & \textit{otherwise.} \end{cases}$$

Interestingly, a new elementary generalization of the congruence (1) of Wolstenholme was only discovered relatively recently by Kimball and Webb [8]. It involves Lucas sequences! If U and V are a pair of Lucas sequences, then the sums $\sum V_t/U_t$ are also $0 \pmod{p^2}$, where t runs over all integers from 1 to $\rho(p) - 1$, where p is a prime at least 5, and $\rho(p)$ denotes the rank of appearance of p in the U sequence, provided, this rank is either $p-1$, p, or $p+1$, that is, p has maximal rank.[1]

This result was shown to hold for the special pair of Lucas sequences consisting of the Fibonacci and of the Lucas numbers in a slightly earlier paper by the same authors [7].

It should briefly be mentioned that this result of Kimball and Webb was further generalized by Pan [13] who showed that, for $w_m > 1$, we have

$$\sum_{t=1}^{m-1} \frac{V_t}{U_t} \equiv \frac{(m^2-1)D}{6} \cdot \frac{U_m}{V_m} \pmod{w_m^2}, \tag{2}$$

where m is an integer ≥ 5, D is the discriminant of the characteristic polynomial associated with the pair of Lucas sequences U and V, and w_m is the largest factor of U_m which is prime to the product $U_2U_3\cdots U_{m-1}$. [2]

We recall that given a pair of integers P and Q, Q nonzero, the two Lucas sequences $U = (U_t)_{t\geq 0}$ and $V = (V_t)_{t\geq 0}$ are second order integral linear recurrences (X_t) that both satisfy the recursion

$$X_{t+2} = PX_{t+1} - QX_t, \quad \text{for all } t. \tag{3}$$

Their two initial terms then fully defines them. We have $U_0 = 0$ and $U_1 = 1$, whereas $V_0 = 2$ and $V_1 = P$. We write $U(P,Q)$ and $V(P,Q)$ when the dependence on P and Q needs to be

[1] The case $\rho(p) = p$ was only considered in the paper [8] when D, the discriminant of the characteristic polynomial of the Lucas sequences, is 0. But the general case can easily be handled as was done in the preprint [1, Thm. 40].

[2] The only case of the Kimball and Webb congruence not implied by (2) is when p is 5 of rank 4. However, defining w_4 as the largest factor of U_4 prime to $3U_2U_3$ would have been sufficient to cover this missing case.

reminded. If the zeros of their characteristic polynomial $x^2 - Px + Q$ are distinct, say α and β, then the t-th terms of the U and V sequences are given by the so-called Binet formulas, i.e.,

$$U_t = \frac{\alpha^t - \beta^t}{\alpha - \beta} \quad \text{and} \quad V_t = \alpha^t + \beta^t. \tag{4}$$

In case $x^2 - Px + Q$ has a double zero α, then the Binet formulas become

$$U_t = t\alpha^{t-1} \quad \text{and} \quad V_t = 2\alpha^t. \tag{5}$$

The rank of appearance $\rho(m)$, or $\rho_U(m)$, of an integer m is the least positive index t such that m divides U_t. It is known to exist for all m prime to Q. The rank of a prime p not dividing Q is either equal to p, or is a divisor of $p \pm 1$. For $(P, Q) = (2, 1)$, 1 is a double zero of $x^2 - Px + Q$. Thus, $U_t = t$ and $V_t = 2$. Applying the theorem of Kimball and Webb to this particular pair of Lucas sequences yields congruence (1).

We restate the main theorem of Kimball and Webb [8], but in a slightly generalized form, as it appeared in Chapter 3 of the paper [1].

Theorem 2. *Let p be a prime at least 5 which is not a factor of Q. Assume the rank ρ of p is maximal. Let k be an integer. Then the sum*

$$\sum_{t \in I_{p,k}} \frac{V_t}{U_t} \text{ is congruent to } 0 \pmod{p^2},$$

where $I_{p,k}$ is the set of integers in the interval $\big(k\rho, (k+1)\rho\big)$.

The purpose of the present paper is to prove a common generalization, Theorem 3 stated hereunder, to both the Leudesdorf and the Kimball-Webb congruences, i.e., a common generalization to Theorems 1 and 2.

Theorem 3. *Let $U(P, Q)$ and $V(P, Q)$ be a pair of Lucas sequences. Let m be an integer of maximal rank with respect to $U(P, Q)$. Then, for all integers k, we have that*

$$S_{m,k}(P, Q) = \sum_{t \in I_{m,k}} \frac{V_t}{U_t} \text{ is congruent to } 0 \pmod{h_m \cdot m^2 / \gcd(m, 3)},$$

where $I_{m,k}$ is the set of integers in the interval $\big(k\rho(m), (k+1)\rho(m)\big)$ that are not multiples of any rank $\rho(p)$ for all primes p dividing m, and where

$$h_m = \begin{cases} 1/2, & \text{if } m = 2^a,\ a \geq 1, \text{ and } \nu_2(P) = 1; \\ 2^\sigma, & \text{if } 2 || m \text{ and } 4 \mid P; \\ 2^\tau, & \text{if } 2 || m,\ P \text{ is odd and } Q \equiv 1 \pmod 4; \\ 8, & \text{if } 4 || m,\ P \text{ is odd and } Q \equiv 3 \pmod 4; \\ 1, & \text{otherwise,} \end{cases}$$

with $\sigma = \nu_2(P) - 2 \geq 0$ and $\tau = \nu_2(P^2 - Q) - 1 \geq 1$, $\nu_2(P)$ and $\nu_2(P^2 - Q)$ being respectively the 2-adic valuations of P and $P^2 - Q$.

In particular, $S_{m,k} \equiv 0 \pmod{m^2 / \gcd(m, 3)}$ if m is not a power of 2 or if $\nu_2(P) \neq 1$.

Example 4. Say $(P,Q) = (1,-1)$, i.e., $U = F$ and $V = L$ are the sequences of Fibonacci and Lucas numbers. We will see that 35 and 500 are two integers of maximal rank with respect to F. Thus, putting $k = 0$ in Theorem 3, we find that

- If $m = 35$, then $\rho(35) = 40$. Hence,

$$\sum_{\substack{t=1 \\ 5\nmid t,\, 8\nmid t}}^{40} \frac{L_t}{F_t} \equiv 0 \pmod{35^2},$$

where the above sum, $S_{m,0}(1,-1)$, contains $40 - (8+5) + 1 = 28$ terms.

- If $m = 500 = 4 \cdot 5^3$, then

$$\sum \frac{L_t}{F_t} \equiv 0 \pmod{8m^2 = 2,000,000},$$

where the sum is over all t's between 1 and $\rho(m) = 6 \cdot 5^3 = 750$ that are prime to 15, and, thus, contains $750 - (250 + 150) + 50 = 400$ terms.

Section 2 of this paper is a short preliminary section where the relevant definitions, and in particular that of a general integer having maximal rank with respect to a Lucas sequence $U(P,Q)$, followed by a few remarks and comments, are given. Section 3 contains the main theorems and their proofs. Theorem 12, generalizes the theorem of Kimball and Webb to prime powers. Theorem 14, which may be viewed as our chief result, is proved via induction on the number of distinct prime factors of an integer m of maximal rank and so Theorem 12 serves as a basis for that proof by induction. Theorem 14 is already a generalization of both Theorems 1 and 2. So we could have ended the paper there. However, it would not have been complete. We wanted a theorem that fully respected the definition we took of an integer of maximal rank. The remaining cases are thus treated in Section 4, but their proofs hinge heavily on the proof of Theorem 14 and are established through a series of lemmas, which, combined with Theorem 14, yield Theorem 3.

The proofs of the paper are all elementary, but assume familiarity with classical properties of Lucas sequences. We refer to Lucas' original work [10] and Chapters 17 and 18 of [11], to [2], [14], to Chapter 4 of [15], and to Chapter 2 of [1], for properties of Lucas sequences used herein.

The letter p invariably denotes a prime number. If m is an integer, then $\rho(m)$, or $\rho_U(m)$, denotes its rank in U. The letter D stands for the discriminant $P^2 - 4Q$ of $x^2 - Px + Q$. If t is a rational number, then $\nu_p(t)$ denotes its p-adic valuation. Alternately, as we did in Theorem 3, we write $p^a || t$ to mean that p^a divides t, but p^{a+1} does not divide t. These divisions take place in the ring A_p. More generally, the congruences in Theorems 1, 2 and 3 and congruences that appear in this paper take place in the ring A_m, where A_m is the subring of the rationals which, when expressed in lowest terms, have a denominator prime to m. That is, $s \equiv t \pmod{m}$ means that s and t are in A_m and that $s - t \in mA_m$. Note that $A_m = A_{m^2} = A_{p_1 \cdots p_r}$, if $p_1, \ldots, p_r$ are the prime factors of m. We will use the well-known fact [6] that $\mathbb{Z}/p^a$ is isomorphic to A_p/p^a, $a \geq 1$, where the isomorphism is derived from the identity embedding of $\mathbb{Z}$ into A_p.

2 Preliminaries

Throughout the paper, we assume that $U = U(P,Q)$ and $V = V(P,Q)$ denote an arbitrary pair of Lucas sequences.

Recall that if m is an integer prime to Q, then $m \mid U_t$ iff $\rho(m) \mid t$. Also, if p is a prime that does not divide Q, then $\rho(p) \mid p-(D|p)$, where $(D|p)$ is 0, if $p \mid D$; 1, if D is a nonzero square (mod p) and -1, otherwise.

We recall a few classical Lucas identities valid for all integers s and t.

$$2U_{s+t} = U_sV_t + U_tV_s, \tag{6}$$

$$2V_{s+t} = V_sV_t + DU_sU_t, \tag{7}$$

$$V_t^2 - DU_t^2 = 4Q^t. \tag{8}$$

It is easy to deduce from (6) and the relations $Q^tV_{-t} = V_t$, $Q^tU_{-t} = -U_t$ that

$$2Q^tU_{s-t} = U_sV_t - U_tV_s. \tag{9}$$

Remark 5. Suppose p is an odd prime not dividing Q. If t is not a multiple of $\rho(p)$, then from (8) we have that the square of the ratio V_t/U_t is well-defined and not congruent to D (mod p).

Our intention is to first generalize Theorem 2 to prime powers, possibly including the primes 2 and 3. Recall that the rank of a prime p is said to be *maximal* if it is $p+1$, p or $p-1$. We wish our generalized theorems to apply to all positive integers m having a certain maximal rank property.

Definition 6. (Maximal Rank) Let p be a prime not dividing Q and a be an integer ≥ 1. We say that the rank of p^a is *maximal* whenever $\rho(p)$ is maximal and $\rho(p^a) = p^{a-1}\rho(p)$. An integer $m \geq 1$ prime to Q is said to have *maximal* rank whenever each prime power dividing m has maximal rank and the ranks of any two prime powers dividing m are coprime.

If m is a prime p, then Definition 6 only requires that $\rho(p)$ be p or $p \pm 1$. However, if $m = p^a$, with $a \geq 2$, has maximal rank, then clearly we also must have $p^1 || U_{\rho(p)}$. Note that if m has maximal rank with respect to $U(P,Q)$, then any divisor n of m has maximal rank with respect to $U(P,Q)$.

Remark 7. It may be useful to observe that if m is the product of prime powers which all have maximal rank with respect to some $U(P,Q)$ and m is either odd, or m and P are both even, then m has maximal rank if and only if $\gcd\big(\rho(p),\rho(q)\big) = 1$, for any two prime factors p and q of m.

Proof. Suppose $\gcd\big(\rho(p), \rho(q)\big) = 1$. We only need to verify that $\rho(p^a)$ and $\rho(q^b)$ are coprime, where $p^a||m$ and $q^b||m$. If p and q are odd, one of them, say q, must have rank equal to q, since $p \pm 1$ and $q \pm 1$ are both even. Thus, $\rho(q^b) = q^b$. So $q \nmid \rho(p)$ and $q \neq p$ yields that $\gcd\big(\rho(p^a), \rho(q^b)\big) = 1$. If p is 2 and q is odd, then, assuming P is even, we have $\rho(p) = 2$ since $U_2 = P$, and thence $\rho(q) = q$. Therefore, $\rho(2^a) = 2^a$ and $\rho(q^b) = q^b$. The converse is immediate. □

The upcoming remark essentially says that if p has maximal rank, the condition $p^2 \nmid U_{\rho(p)}$ suffices for all p^a, $a \geq 1$, to have maximal rank. Note that if U is the Fibonacci sequence, then the search for a Wall-Sun-Sun prime, i.e., a prime p such that p^2 divides $U_{\rho(p)}$, has gathered attention, but to this date none is known to exist and there does not exist any below 2×10^{14} [12].

Remark 8. Let $p \nmid Q$ be a prime of maximal rank such that $p^2 \nmid U_{\rho(p)}$. Additionally, we assume P is even, if p is 2. Then p^a has maximal rank for all $a \geq 1$.

Proof. By Theorem 9 of [1], the rank of p^a is equal to $p^{a-1}\rho(p)$, if p is odd. Suppose $p = 2$. Since $U_1 = 1$, $U_2 = P$ and P is even, we have $\rho(2) = 2$. By hypothesis, $4 \nmid U_{\rho(2)}$, i.e., $4 \nmid P$, and Q is odd. Therefore, $8 \mid D = P^2 - 4Q$. By identity (8), $\nu_2(V_t) = 1$ for all integers t's. Thus, the 2-adic valuation of $U_{2t} = U_t V_t$ is one more than that of U_t. So by induction we obtain that $\rho(2^a) = 2^{a-1}\rho(2) = 2^a$. □

With the help of Lemma 15, we give the full list of integers of maximal rank with respect to the Fibonacci sequence.

Example 9. An integer $m \geq 1$ has maximal rank with respect to the Fibonacci sequence $F = U(1, -1)$ iff it has the form

$$2^a\, 5^b\, p^c,$$

where p is a prime 3 (mod 4) of rank $\rho(p) = p \pm 1$, not a Wall-Sun-Sun prime in case $c \geq 2$, and where $a \in \{0, 1, 2\}$, $b \geq 0$, $c \geq 0$ with

- $c = 0$, if $a = 2$;
- $3 \nmid \rho(p)$, if $a = 1$ and $c \geq 1$;
- $5 \nmid \rho(p)$, if $b \geq 1$ and $c \geq 1$.

Artin's conjecture states that an integer a, not a square, with $|a| \geq 2$, is a primitive root modulo infinitely many primes. In fact, it has been conditionally proved that such primes have a positive density [5]. Similarly here, since Q is not a square, it is expected that a positive proportion of the primes 3 (mod 4) have maximal ranks in F. In fact, 3, 7, 11, 19, 23, 31 and 43 all have maximal ranks, 47 being the smallest prime 3 (mod 4) with rank less than $p - 1$. For all primes p that are 1 (mod 4), we have that $p \mid U_{(p-1)/2}$ or $p \mid U_{(p+1)/2}$.

Definition 10. ($I_{m,k}$ and $S_{m,k}$) Given an integer $m \geq 1$ and an integer k, we define $I_{m,k}$ as the set of integers that lie in the interval $\big[k\rho(m), (k+1)\rho(m)\big]$ and are not a multiple of any $\rho(p)$, for all primes p dividing m. Then $S_{m,k}$ will denote the sum of all V_t/U_t in A_m as t varies through $I_{m,k}$. We write $I_{m,k}(P, Q)$ or $S_{m,k}(P, Q)$ if the dependence on (P, Q) needs to be specified.

In coining the two definitions 6 and 10, we had two constraints in our mind. In Leudesdorf's Theorem 1, the sum involved is $S_{m,0}(2,1)$. That sum goes up to m, which is viewed as the rank of m in $U_t = t$. Thus, if we wanted a theorem that generalizes Theorem 1, then $I_{m,0}$ had to go up to $\rho(m)$. Actually, considering sums that go up to the least common multiple of the ranks of the prime powers dividing an integer m would also reduce to the right sums when $U_t = t$. However, generally these sums are not $0 \pmod{m^2}$.[3] Also we wanted the arguments used in proving Theorem 2 to remain valid, which meant that $S_{m,k}$ should have about m terms. These observations guided us in defining the notion of maximal rank.

Lemma 11. *Let k be an integer. Let m be an integer ≥ 1 prime to Q. If m is odd, then all ratios V_t/U_t are distinct (mod m) as t varies through $I_{m,k}$. If m is even and $2||P$, then all ratios $V_t/(2U_t)$ are distinct (mod m) as t varies through $I_{m,k}$.*

Proof. Assume first m is odd. If s and t are distinct integers in $I_{m,k}$, then U_{s-t} is not divisible by m. Thus, dividing (9) through by U_sU_t, we get that

$$\frac{V_t}{U_t} - \frac{V_s}{U_s} = 2Q^t \frac{U_{s-t}}{U_sU_t}. \tag{10}$$

Since the right-hand term of (10) is not $0 \pmod{m}$, all ratios V_t/U_t are pairwise incongruent modulo m as t varies through $I_{m,k}$. For the case m even, note that $P = 2P'$ with P' odd. Since $D = 4(P'^2 - Q)$, 8 divides D. We have $V_t^2 - DU_t^2 = 4Q^t$, so each V_t is even and the ratios $V_t/(2U_t)$ do belong to the ring A_m for $t \in I_{m,k}$. The reasoning is then similar to that of m odd. $\square$

3 Main Theorems and Proofs.

Theorem 12. *Let $U(P,Q)$ and $V(P,Q)$ be a pair of Lucas sequences. Let p be a prime number. Suppose p^a has maximal rank with respect to $U(P,Q)$, where P is even and not divisible by 4 in case p is 2. Then for all integers k*

$$S_{p^a,k} = \sum_{t \in I_{p^a,k}} \frac{V_t}{U_t} \ \text{ is congruent to } 0 \pmod{p^c},$$

where

$$c = \begin{cases} 2a, & \text{if } p \geq 5; \\ 2a-1, & \text{if } p = 2 \text{ or } 3. \end{cases}$$

Proof. Fix an integer k. Note that $I_{p^a,k}$ contains $p^{a-1}\rho(p) - p^{a-1} = p^{a-1}\big(\rho(p) - 1\big)$ integers. By convention, all unmarked sums appearing in the proof are taken over the set $I_{p^a,k}$, and thus contain $p^{a-1}\big(\rho(p)-1\big)$ terms. Denote $(2k+1)p^{a-1}\rho(p)$ by b. Since the rank of p^a is $p^{a-1}\rho(p)$, we have that p^a divides $U_{p^{a-1}\rho(p)}$ and that U_b is at least divisible by p^a. By (6),

$$2S_{p^a,k} = \sum \left(\frac{V_t}{U_t} + \frac{V_{b-t}}{U_{b-t}} \right) = 2\sum \frac{U_b}{U_tU_{b-t}}.$$

[3] For instance, 3 and 7 have maximal ranks in the Fibonacci sequence and the least common multiple of their ranks is 8. But $\sum_{t=1}^{8} L_t/F_t$, $(4 \nmid t)$, is 0 (mod 21), 6 (mod 9) and 14 (mod 49).

Suppose p is odd. Hence, it suffices to show that $\sum 2/(U_tU_{b-t})$ is divisible by p^d, where $d = a$ if $p > 3$, and $d = a - 1$ if $p = 3$. By (8) with $t = b$, $\gcd(U_b, V_b)$ divides $2Q^{\lfloor b/2 \rfloor}$, so that p does not divide V_b. Thus, it also suffices to show that

$$S_1 := \sum \frac{2V_b}{U_tU_{b-t}}$$

is divisible by p^d. Now, by (7), S_1 is equal to

$$\sum \frac{V_tV_{b-t}}{U_tU_{b-t}} \; + \; Dp^{a-1}\big(\rho(p) - 1\big).$$

But

$$\sum \frac{V_tV_{b-t}}{U_tU_{b-t}} = \sum \frac{U_tU_{b-t}V_tV_{b-t}}{(U_tU_{b-t})^2} = \frac{1}{2}\sum \frac{(U_tV_{b-t} + U_{b-t}V_t)^2}{(U_tU_{b-t})^2} - \sum \left(\frac{V_t}{U_t}\right)^2.$$

In the above final expression, the numerators of the terms in the first sum are all equal to $4U_b^2$ by (6). Since p^a divides U_b, we have that p^d divides S_1, if and only if, p^d divides

$$S_2 := Dp^{a-1}\big(\rho(p) - 1\big) - S_3,$$

where $S_3 := \sum (V_t/U_t)^2$.

If $\rho(p)$ is $p + 1$, then S_2 is congruent to $-S_3 \pmod{p^a}$. But since by Lemma 11 the p^a rational numbers V_t/U_t that appear in S_3 are all distinct $0 \pmod{p^a}$, we have that

$$S_3 \equiv \sum_{t=1}^{p^a} t^2 = \frac{p^a(p^a+1)(2p^a+1)}{2 \cdot 3} \pmod{p^a},$$

which yields that

$$S_3 \equiv 0 \pmod{p^d}.$$

If $\rho(p)$ is p, then p divides D. Thus, again, $S_2 \equiv -S_3 \pmod{p^a}$. Since p has odd rank, say by Theorem 10 in [1], no term of the V sequence is divisible by p. Thus, the $p^a - p^{a-1}$ ratios V_t/U_t that appear in S_3, being all distinct $(\mathrm{mod}\ p^a)$, are all the invertible elements of the ring A_p/p^a. As they form a cyclic multiplicative group generated by, say, g, we have

$$S_3 \equiv \sum_{k=0}^{\varphi(p^a)-1} g^{2k} = \frac{g^{2\varphi(p^a)} - 1}{g^2 - 1} \pmod{p^a},$$

where φ denotes Euler's totient function. For odd primes p, any primitive root $(\mathrm{mod}\ p^a)$ reduces to a primitive root $(\mathrm{mod}\ p)$. Therefore, the order of $g \pmod{p}$ is $p - 1$ and, thus $p \mid g^2 - 1$ iff $p - 1 \mid 2$, i.e., iff $p = 3$. But if $p = 3$ and $a \geq 2$, then g being a primitive root $(\mathrm{mod}\ 9)$, the quantity $g^2 - 1$ is divisible by 3, but not by 9. If $p = 3$ and $a = 1$, then $d = 0$. Therefore, for all cases, we have

$$S_3 \equiv \; 0 \pmod{p^d}.$$

If $\rho(p)$ is $p-1$, then the set $I_{p^a,k}$ is made up of p^{a-1} integer intervals of length $p-2$. Indeed, integers in $I_{p^a,k}$ are not divisible by $\rho(p)$, i.e., by $p-1$. As t varies through each such interval all V_t/U_t are distinct (mod p), and are not equal to any of the two square roots of D (mod p) by Remark 5. Thus, the summands $(V_t/U_t)^2$ in S_3 take the value 0 once and every nonzero quadratic residue (mod p) twice, except D, on each interval of length $p-2$ of $I_{p^a,k}$. Thus, as t runs through $I_{p^a,k}$ and since all V_t/U_t are distinct (mod p^a), none of the summands $(V_t/U_t)^2$ of S_3 is equal to any of the residues D, $D+p$, $D+2p, \ldots, D+(p^{a-1}-1)p$ (mod p^a). Thus,

$$S_3 \equiv \sum_{i=1}^{p^a} i^2 - 2\sum_{j=1}^{p^{a-1}}(D+jp) \equiv\ 0 - 2p^{a-1}D \pmod{p^d}.$$

Therefore, $S_2 = Dp^{a-1}(p-2) - S_3 \equiv\ -2Dp^{a-1} + 2p^{a-1}D = 0 \pmod{p^d}$.

Suppose $p = 2$. The symbols S_1, S_2 and S_3 refer to the same sums we had defined in the case where p was odd. Since P is even and $U_2 = P$, $\rho(2) = 2$ and $b = (2k+1)2^a$. As seen in proving Remark 8, $\nu_2(U_{2^a}) = a$ and so we also have $\nu_2(U_b) = a$. Therefore, as $S_{2^a,k} = \sum \frac{U_b}{U_tU_{b-t}}$, we have

$$\nu_2(S_{2^a,k}) = a + \nu_2\left(\sum \frac{1}{U_tU_{b-t}}\right) = a + \nu_2\left(\sum \frac{2V_b}{U_tU_{b-t}}\right) - 2,$$

since, as shown in Remark 8, $\nu_2(V_b) = 1$. Thus, we need to show that $\nu_2(S_1) \geq a+1$. In fact, we will see that $\nu_2(S_1) = a+1$ so that $\nu_2(S_{2^a,k})$ is exactly $2a-1$ for all integers k. Because $\frac{1}{2}(4U_b^2)$ is divisible by 2^{2a+1}, which is $> 2^{a+1}$, $\nu_2(S_1) = a+1$ iff $\nu_2(S_2) = a+1$. Since $D = 4(P'^2 - Q)$, where $P = 2P'$ and P' is odd, $8 \mid D$. Therefore, $\nu_2(S_2)$ is $a+1$ iff $\nu_2(S_3) = a+1$. But $S_3 = 4S_4$, where $S_4 = \sum \frac{V_t^2}{4U_t^2}$. The 2^{a-1} terms $V_t/2U_t$ are all distinct (mod 2^a), by Lemma 11, and each such term is a unit of the ring A_2, by the proof of Remark 8. Therefore,

$$S_4 \equiv \sum_{t=1}^{2^{a-1}} (2t-1)^2 \pmod{2^a}.$$

But $\sum_{t=1}^{N}(2t-1)^2 = 4(N-1)N(N+1)/3 - N$ so $2^{a-1}||S_4$. Since $S_3 = 4S_4$, we have $\nu_2(S_3) = a+1$ as required. □

Remark 13. Under the hypotheses of Theorem 12, we have actually shown that the sums $S_{2^a,k}$ have 2-adic valuation exactly equal to $2a-1$, for all integers k.

We are ready to move on to our main result.

Theorem 14. *Let $U(P,Q)$ and $V(P,Q)$ be a pair of Lucas sequences. Let m be an integer of maximal rank with respect to $U(P,Q)$. If m is even, then we make the additional hypothesis that P is even and not divisible by 4. Then for all integers k*

$$S_{m,k}(P,Q) = \sum_{t\in I_{m,k}} \frac{V_t}{U_t} \ \textit{ is congruent to }\ 0 \pmod{m^2/d_m},$$

where $I_{m,k}$ is the set of integers in the interval $\big(k\rho(m),(k+1)\rho(m)\big)$ that are not multiples of any rank $\rho(p)$ for all primes p dividing m, and where

$$d_m = \begin{cases} 2, & \text{if } m = 2^a,\ a \geq 1; \\ 3, & \text{if } 3 \mid m; \\ 1, & \text{otherwise.} \end{cases}$$

Proof. We proceed by induction on $\omega(m)$, where ω denotes the distinct prime factors counting function. More precisely, our inductive hypothesis at level i, $i \geq 1$, says that for all integers k, all integers $m \geq 1$ with $\omega(m) = i$ and all Lucas sequences $U = U(P,Q)$ with respect to which m satisfies the hypotheses of Theorem 14, the sum $S_{m,k}(P,Q)$ is congruent to $0 \pmod{m^2/d_m}$.

The case $i = 1$ was established in Theorem 12, so we assume that $i \geq 2$ and that the result holds for integers having $i-1$ distinct prime factors. To prove the inductive hypothesis at level i, we establish two properties (11) and (12) which together clearly suffice to prove the inductive step. The first property says that

$$\text{if } m = p^a n, \text{ then } n^2/d_n \text{ divides } S_{m,k}, \tag{11}$$

where p is a prime that does not divide n and $a \geq 1$. Note that (11) is sufficient to prove the inductive step if m is odd, but not if m is even, unless we know the theorem holds for even integers at level $i = 2$. Thus, in addition, we prove that

$$\text{if } m = 2^a q^b, \text{ then } 2^{2a} \text{ divides } S_{m,k}, \tag{12}$$

where q is an odd prime, a and $b \geq 1$.

We begin by establishing (11) inductively. To this end, we note that

$$S_{m,k} = S^* - S^{**},$$

where

$$S^* = \sum_{j=0}^{\rho(p^a)-1} \sum_{\substack{t=k\rho(m)+j\rho(n) \\ \rho(q)\nmid t \text{ if } q|n}}^{k\rho(m)+(j+1)\rho(n)} \frac{V_t}{U_t} \qquad \text{and} \qquad S^{**} = \sum_{\substack{t=k\rho(m) \\ \rho(p)\,|\,t \\ \rho(q)\nmid t,\,\forall q|n}}^{(k+1)\rho(m)} \frac{V_t}{U_t}, \tag{13}$$

and the letter q stands for a prime. Moreover, we have

$$S^* = \sum_{j=0}^{\rho(p^a)-1} S_{n,j+k\rho(p^a)}. \tag{14}$$

Each inner sum $S_{n,j+k\rho(p^a)}$ in S^* is, by the inductive hypothesis, divisible by n^2/d_n, so we are left with showing that S^{**} is also divisible by n^2/d_n. But

$$S^{**} = \sum_{\substack{t=k\rho(n)p^{a-1} \\ \rho(q)\nmid t,\,\forall q|n}}^{(k+1)\rho(n)p^{a-1}} \frac{V_{\rho(p)t}}{U_{\rho(p)t}} = U_{\rho(p)}^{-1} \sum_{j=kp^{a-1}}^{(k+1)p^{a-1}-1} S_{n,j}\big(V_{\rho(p)}, Q^{\rho(p)}\big). \tag{15}$$

In (15), the sum $S_{n,j}\big(V_{\rho(p)}, Q^{\rho(p)}\big)$ is associated with the pair of Lucas sequences attached to the recursion $x^2 - V_{\rho(p)}x + Q^{\rho(p)}$. Indeed, we have

$$V_{\rho(p)t}(P,Q) = V_t(P',Q') \;\text{ and }\; U_{\rho(p)t}(P,Q) = U_t(P',Q') \cdot U_{\rho(p)}(P,Q), \tag{16}$$

where $P' = V_{\rho(p)}(P,Q)$ and $Q' = Q^{\rho(p)}$. Identities (16) may be derived from the Binet formulas for U_t and V_t whether the discriminant $P^2 - 4Q$ is zero or nonzero. For instance, suppose $x^2 - Px + Q = (x-\alpha)^2$. Then $U_t(P,Q) = t\alpha^{t-1}$ and denoting $\rho(p)$ by ρ we have

$$\begin{aligned} U_{\rho t}(P,Q) &= \rho t\alpha^{\rho t-1} = \rho t\alpha^{\rho(t-1)+(\rho-1)} \\ &= \rho\alpha^{\rho-1} \cdot t(\alpha^{\rho})^{t-1} \\ &= U_{\rho}(P,Q) \cdot U_t(P',Q'). \end{aligned}$$

By the inductive hypothesis n^2/d_n divides each sum $S_{n,j}(P',Q')$, for all j's, provided we check, on the one hand, that n has maximal rank with respect to $U' = U(P',Q')$ and, on the other, in case n is even, that $\nu_2(P') = 1$.

Since m is prime to Q, n is prime to Q'. Let q be a prime factor of n, $\rho(q)$ be its rank in $U = U(P,Q)$ and $\rho'(q)$ its rank in $U' = U(P',Q')$, where as above $\rho(p)$ is the rank of p in U. By hypothesis, $\rho(q)$ and $\rho(p)$ are coprime so that $q \nmid U_{\rho(p)}$. Thus, as $U_{\rho(p)t} = U_{\rho(p)} \cdot U'_t$, we have that $q \mid U'_t$ iff $q \mid U_{\rho(p)t}$ iff $\rho(q) \mid \rho(p)t$ iff $\rho(q) \mid t$. Thus, $\rho(q) = \rho'(q)$. We conclude that the rank of q in U' is maximal. Similarly, since $\rho(q^s) = q^{s-1}\rho(q)$ is also prime to $\rho(p)$, the ranks of q^s in U and in U' are identical for all $s \geq 2$. Therefore, if $q^{\alpha}||m$, then, as $\rho(q^{\alpha})$ exists and is equal to $q^{\alpha-1}\rho(q)$, we have $\rho'(q^{\alpha}) = q^{\alpha-1}\rho'(q)$. That is, q^{α} has maximal rank in U'. Moreover, distinct prime factors of n have coprime ranks in U'.

Suppose n is even. Then m is even. Hence, Q is odd and $\nu_2(P) = 1$, which, as proved in Remark 8, implies that $\nu_2(V_t) = 1$ for all integers t. But $P' = V_{\rho(p)}$.

Thus, since each prime factor q of n is prime to $U_{\rho(p)}$, we deduce that S^{**} is divisible by n^2/d_n. We have proved (11).

To prove (12), we assume $i = 2$ and 'recycle' the proof of (11). So given $m = 2^a q^b$ we have, by (11), that $2^{2a-1}q^{2b}/d_q = m^2/(2d_m)$ divides $S_{m,k}$. Reexamining the proof of (11) with $p = q$, we will show that in fact 2^{2a} divides $S_{m,k}$. By Remark 13, each of the $\rho(q^b)$ sums $S_{2^a,j+k\rho(q^b)}$ in (14) is divisible by 2^{2a-1}, but not by 2^{2a}. But, by (15), we see that S^{**} is also the sum of q^{b-1} sums each of which is exactly divisible by 2^{2a-1}. Therefore, $S_{m,k}$ is the sum of $\rho(q^b) + q^{b-1}$ terms each divisible exactly by 2^{2a-1}. Thus, it suffices to check that $\rho(q^b) + q^{b-1}$ is even. But $\rho(2) = 2$, and so $\rho(q)$ must be odd. As the rank of q is maximal, it must be that $\rho(q) = q$. Hence, $\rho(q^b) + q^{b-1} = q^{b-1}(q+1)$. $\square$

4 The Remaining Cases

Theorem 14 clearly contains Theorem 2, but it also implies Theorem 1. Indeed, for $(P,Q) = (2,1)$, we have $U_t = t$ and $V_t = 2$, for all t's. In particular, $\nu_2(P) = 1$ and all integers $m \geq 1$ have maximal rank. Say, for instance, that $3 \mid m$. Then, by Theorem 14, $\sum_{t \in I_{m,0}} 2/t \equiv$

0 (mod $m^2/3$), which implies

$$\sum_{\substack{t=1\\ \gcd(t,m)=1}}^{m} 1/t \equiv\ 0 \pmod{m^2/\gcd(m,6)},$$

as $\gcd(t,m)=1$ iff $\rho(p)=p\nmid m$ for all primes p dividing m.

But Theorem 14 does not apply to even integers having maximal rank in $U(P,Q)$, if either $4\mid P$, or P is odd. The next lemmas treat those missing cases, and, combined with Theorem 14, they yield Theorem 3 stated in the introduction.

The first lemma fully describes when powers of 2 have maximal rank.

Lemma 15. *Assume Q is odd. Then 2^a, $a\ge 1$, has maximal rank in $U(P,Q)$ if and only if*

$$\begin{cases} a=1, & \text{if } 4\mid P, \text{ or if } P \text{ is odd and } Q\equiv 1 \pmod 4;\\ a=1 \text{ or } 2, & \text{if } P \text{ is odd and } Q\equiv 3 \pmod 4;\\ a\ge 1, & \text{if } P\equiv 2 \pmod 4.\end{cases}$$

Proof. Since $U_2=P$ and $U_3=P^2-Q$, either P is even and $\rho(2)=2$, or P is odd and $\rho(2)=3$. Thus, 2^a has maximal rank for $a=1$.

If $4\mid P$, or if P is odd and $Q\equiv 1 \pmod 4$, then $\rho(4)=\rho(2)$. By (8), if U_t is even, then V_t is even. Since $U_{2t}=U_tV_t$, we have $\nu_2(U_{2t})\ge 1+\nu_2(U_t)$. Therefore, since $\rho(4)=\rho(2)$, $\rho(2^a)<2^{a-1}\rho(2)$ for all $a\ge 2$.

If P is odd and $Q\equiv 3 \pmod 4$, then $\rho(2)=3$ and $\rho(4)=6$. Thus, 4 has maximal rank. However, $U_6=U_2U_3(P^2-3Q)$ and $4\mid P^2-3Q$, so $8\mid U_6$. Hence, $\rho(8)=\rho(4)$ and $\rho(2^a)<2^{a-1}\rho(2)$, for all $a\ge 3$.

The case $P\equiv 2 \pmod 4$ was taken care of in Remark 8. □

Lemma 16. *Let $U(P,Q)$ and $V(P,Q)$ be a pair of Lucas sequences, where P is divisible by 4 and Q is odd. Let m be an even integer of maximal rank with respect to $U(P,Q)$. Then for all integers k*

$$S_{m,k}(P,Q)\equiv\ 0 \pmod{2^\sigma m^2/\gcd(m,3)},$$

where $\sigma=\nu_2(P)-2$.

Proof. By Lemma 15, m is not divisible by 4. So we write $m=2n$ with n odd. Since $\rho(2)=2$, all odd prime factors p of m satisfy $\rho(p)=p$. As in proving Theorem 14, we carry an induction on $i=\omega(m)$, where the inductive hypothesis at level i assumes the lemma to hold for all integers m with $\omega(m)=i$, all pairs (P',Q'), $4\mid P'$ and Q' odd, with respect to which m has maximal rank in $U(P',Q')$ and all integers k. If $i=1$, that is, if $m=2$, then $S_{2,k}=V_{2k+1}/U_{2k+1}$. An easy induction using (3) yields that $\nu_2(V_{2t})=1$ and $\nu_2(V_{2t+1})=\nu_2(P)$, for all integers t. Hence, $2^{\nu_2(P)}||S_{2,k}$. But $2^{\nu_2(P)}=2^\sigma m^2$. Assume that $i\ge 2$ and that the inductive hypothesis holds at level $i-1$. We decompose $S_{m,k}$ into the difference of S^* and S^{**} as we did in the proof of Theorem 14 by choosing a prime p that divides m. If p is 2, then, by Theorem 14, both the inner sums $S_{n,j+2k}(P,Q)$ of S^* in (14) and the inner sums $S_{n,j}(P',Q')$ of S^{**} in (15) are divisible by n^2/d_n, where $d_n=\gcd(n,3)$.

But $\gcd(n,3) = \gcd(m,3)$ so $n^2/\gcd(m,3)$ divides $S_{m,k}$. It remains to see that $2^{\nu_2(P)}$ divides $S_{m,k}$. If p is odd, then put $\ell = m/p^a$, where $a = \nu_p(m)$. The inner sums $S_{\ell,j+k\rho(p)}(P,Q)$ of S^* are now divisible by $2^\sigma \ell^2/\gcd(\ell,3)$, and by $2^{\nu_2(P)}$ in particular, by the inductive hypothesis. The inner sums $S_{\ell,j}(P',Q')$ are divisible by $2^{\nu_2(P')}$ by the inductive hypothesis, which is applicable since $4 \mid P'$ and Q' is odd. But $P' = V_{\rho(p)} = V_p$ and $\nu_2(V_p) = \nu_2(P)$, since p is odd. Hence, $S_{m,k}$ is divisible by $2^\sigma m^2/\gcd(m,3)$. □

Lemma 17. *Let $U(P,Q)$ and $V(P,Q)$ be a pair of Lucas sequences, where P is odd and Q is congruent to* 1 (mod 4)*. Let m be an even integer of maximal rank with respect to $U(P,Q)$. Then for all integers k*

$$S_{m,k}(P,Q) \equiv 0 \pmod{2^\tau m^2/\gcd(m,3)},$$

where $\tau = \nu_2(P^2 - Q) - 1 \geq 1$.

Proof. One may carry a successful induction that closely follows that of the proof of Lemma 16. Note that $4 \nmid m$ and that $\rho(2) = 3$. If $m = p^a\ell$, ℓ even, then by induction the sums $S_{\ell,j}(P',Q')$ in S^{**} are divisible by $2^\tau \ell^2/\gcd(\ell,3)$. Indeed, $2 \mid V_t$ iff $3 \mid t$. Thus, since $P' = V_{\rho(p)}$ and $\rho(2) \nmid \rho(p)$, P' is odd. Moreover, $Q' = Q^{\rho(p)} \equiv 1 \pmod 4$. If $m = 2n$, then, by Theorem 14 applied to the inner sums in both S^* and S^{**}, n^2/d_n divides $S_{m,k}$, where d_n was defined in Theorem 14.

For the base step of the induction, note that if $\omega(m) = 1$, then $m = 2$. So $I_{2,k} = \{3k+1, 3k+2\}$ and $S_{2,k} = 2U_{6k+3}/U_{3k+1}U_{3k+2}$. Therefore, we have $\nu_2(S_{2,k}) = \nu_2\big(2U_3\big) = 2+\tau$. Indeed, $U_{3(2k+1)} = U_3 \cdot U'_{2k+1}$, where $U' = U(V_3, Q^3)$, and $U'_t \pmod 2 = 0,1,0,1,0,1,\cdots$ $(t \geq 0)$, since V_3 is even. □

Lemma 18. *Let $U(P,Q)$ and $V(P,Q)$ be a pair of Lucas sequences, where P is odd and Q is congruent to* 3 (mod 4)*. Let m be an even integer not divisible by* 4 *of maximal rank with respect to $U(P,Q)$. Then for all integers k*

$$S_{m,k}(P,Q) \equiv 0 \pmod{m^2/\gcd(m,3)}.$$

Proof. An induction very similar to those used in proving Lemmas 16 and 17 works fine. Note however that besides Theorem 14, Lemma 17 also comes into play. Indeed, if $m = p^a\ell$, p an odd prime not dividing ℓ, then the sums $S_{\ell,j}$ in S^{**} are associated with a Lucas sequence $U(P',Q')$, where P' is odd, but $Q' = Q^{\rho(p)}$ is congruent to $1 \pmod 4$, if $\rho(p)$ is even. The base step of the induction corresponds to $m = 2$ and, as in the proof of Lemma 17, we have $\nu_2(S_{2,k}) = \nu_2(2U_3)$. However, $U_3 = P^2 - Q$ is even, but not divisible by 4. □

Lemma 19. *Let $U(P,Q)$ and $V(P,Q)$ be a pair of Lucas sequences, where P is odd and Q is congruent to* 3 (mod 4)*. Let m be an integer divisible by* 4 *of maximal rank with respect to $U(P,Q)$. Then for all integers k*

$$S_{m,k}(P,Q) \equiv 0 \pmod{8m^2}.[4]$$

[4] Thus, 2^7 divides $S_{m,k}$. Unless we refine further the hypotheses on P and Q, the exponent 7 is optimal. For instance, $S_{4,0}(1,-1) = \frac{128}{15}$.

Proof. A proof by induction on $i = \omega(m)$ of the same model as in the three previous lemmas works fine. The rank of 4 is 6. Since the rank of 3 must be 2, 3 or 4, and none of these is prime to 6, $3 \nmid m$. Writing m as $4n$ with n odd, we find that n^2 divides $S_{m,k}$ by Theorem 14. Thus, we are left with seeing that 2^7 divides $S_{m,k}$. Write m as $p^a\ell$, where p is a prime ≥ 5 and $p \nmid \ell$. We have that $4 \mid \ell$ and that the inner sums $S_{\ell,j+k\rho(p^a)}$ in S^* are divisible by $8\ell^2$ and by 2^7 in particular, using the inductive hypothesis. How about the inner sums $S_{\ell,j}(P', Q')$ of S^{**}? Note that $\rho(2)$ is 3. So m being of maximal rank, $3 \nmid \rho(p)$. But $2 \mid V_t$ iff $3 \mid t$. So $P' = V_{\rho(p)}$ is odd. In fact, as $\rho(4) = 6$, $\rho(p)$ must also be odd, that is to say, $\rho(p) = p$. Thus, $Q' = Q^{\rho(p)} \equiv 3 \pmod 4$. The inductive hypothesis yields that S^{**} is divisible by 2^7.

We have not checked the initial step of the induction, i.e., the case $m = 4$. Note that $I_{4,k} = \{6k+1, 6k+2, 6k+4, 6k+5\}$. Combining, on one hand, the first and fourth terms of $S_{4,k}$, and, on the other hand, the middle ones, yields

$$S_{4,k} = \frac{2U_{12k+6}}{U_{6k+1}U_{6k+5}} + \frac{2U_{12k+6}}{U_{6k+2}U_{6k+4}}.$$

Hence, $\nu_2(S_{4,k}) = \nu_2(2U_6) + \nu_2(U_{6k+2}U_{6k+4} + U_{6k+1}U_{6k+5})$. But $U_6 = U_2U_3(P^2 - 3Q) = P(P^2 - Q)(P^2 - 3Q)$, so that

$$\nu_2(2U_6) = 2 + \nu_2(P^2 - 3Q) \geq \begin{cases} 5, & \text{if } Q \equiv 3 \pmod 8; \\ 4, & \text{if } Q \equiv 7 \pmod 8. \end{cases} \tag{17}$$

Since $\rho(8) = 6$, we have $U_{t+6} \equiv U_7U_t \pmod 8$ for all $t \geq 0$. Indeed, the congruence holds for $t = 0$ and $t = 1$, and, by (3), it must hold for all t's. Thus,

$$U_{6k+2}U_{6k+4} + U_{6k+1}U_{6k+5} \equiv U_7^{2k}(U_2U_4 + U_1U_5) \pmod 8.$$

A direct calculation gives $U_2U_4 + U_1U_5 = 2P^4 - 5P^2Q + Q^2 \equiv 3(Q+1) \pmod 8$. Therefore,

$$\nu_2(U_{6k+2}U_{6k+4} + U_{6k+1}U_{6k+5}) \geq \begin{cases} 2, & \text{if } Q \equiv 3 \pmod 8; \\ 3, & \text{if } Q \equiv 7 \pmod 8, \end{cases}$$

which, combined with (17), yields that $\nu_2(S_{4,k}) \geq 7$ for all integers k. □

5 Acknowledgments

We thank the two referees for time spent reading this paper and writing up comments and suggestions. One of the referees pointed out reference [13].

References

[1] Christian Ballot, Lucas sequences with cyclotomic root field, submitted preprint, 120 pages.

[2] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.*, **15**, (1913–14), 30–48, 49–70.

[3] S. Chowla, Leudesdorf's generalization of Wolstenholme's theorem, *J. London Math. Soc.*, **9** (1934), 246.

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

[5] C. Hooley, On Artin's conjecture, *J. reine angew. Math.* **225** (1967), 209–220.

[6] G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

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

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

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

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

[11] Édouard Lucas, *Théorie des Nombres*, Librairie scientifique et technique Albert Blanchard, 1961.

[12] Richard J. McIntosh and Eric L. Roettger, A search for Fibonacci-Wieferich and Wolstenholme primes, *Math. Comp.*, **76** (2007), 2087–2094.

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

[14] Paulo Ribenboim, The Fibonacci numbers and the Artic Ocean, Proceedings of the 2nd Gauss Symposium. Conference A: *Mathematics and Theoretical Physics*, de Gruyter, 1995, pp. 41–83.

[15] Hugh C. Williams, *Édouard Lucas and Primality Testing*, Wiley, 1998.

[16] Joseph Wolstenholme, On certain properties of prime numbers, *Quarterly J. Pure Applied Math.*, **5** (1862), 35–39.

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

Received June 6 2012; revised version received October 8 2012. Published in *Journal of Integer Sequences*, October 8 2012. Minor typographical corrections, November 24 2013.

Return to Journal of Integer Sequences home page.