Journal of Integer Sequences, Vol. 13 (2010),
Article 10.2.4

The Terms in Lucas Sequences Divisible by Their Indices

Chris Smyth
School of Mathematics and Maxwell Institute for Mathematical Sciences
University of Edinburgh
James Clerk Maxwell Building
King's Buildings
Mayfield Road
Edinburgh EH9 3JZ
United Kingdom
c.smyth@ed.ac.uk

Abstract

For Lucas sequences of the first kind $(u_n)_{n\geq 0}$ and second kind $(v_n)_{n\geq 0}$ defined as usual by $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, $v_n = \alpha^n + \beta^n$, where α and β are either integers or conjugate quadratic integers, we describe the sets $\{n \in \mathbb{N} : n \text{ divides } u_n\}$ and $\{n \in \mathbb{N} : n \text{ divides } v_n\}$. Building on earlier work, particularly that of Somer, we show that the numbers in these sets can be written as a product of a so-called *basic* number, which can only be 1, 6 or 12, and particular primes, which are described explicitly. Some properties of the set of all primes that arise in this way is also given, for each kind of sequence.

1 Introduction

Given integers P and Q, let α and β be the roots of the equation

$$x^2 - Px + Q = 0.$$

Then the well-known *Lucas sequence of the first kind* (or *generalised Fibonacci sequence*) $(u_n)_{n\geq 0}$ is given by $u_0 = 0, u_1 = 1$ and $u_{n+2} = Pu_{n+1} - Qu_n$ for $n \geq 0$, or explicitly by Binet's formula

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

when $\Delta = (\alpha - \beta)^2 = P^2 - 4Q \neq 0$, and $u_n = n\alpha^{n-1}$ when $\Delta = 0$. In this latter case α is an integer, and so n divides u_n for all $n \geq 1$. In Theorem 1 below we describe, for all pairs (P, Q), the set $S = S(P, Q)$ of all $n \geq 1$ for which n divides u_n.

Corresponding to Theorem 1 we have a similar result (Theorem 12 below) for the *Lucas sequence of the second kind* $(v_n)_{n\geq 0}$, given by $v_0 = 2, v_1 = P$ and $v_{n+2} = Pv_{n+1} - Qv_n$ for $n \geq 0$, or explicitly by the formula

$$v_n = \alpha^n + \beta^n,$$

finding the set $T = T(P, Q)$ of all $n \geq 1$ for which n divides v_n. The results for the set T are given in Section 4.

For $n \in S$, define $\mathcal{P}_{S,n}$ to be the set of primes p such that $np \in S$. We call an element n of S *(first kind) basic* if there is no prime p such that n/p is in S. We shall see that, for given P, Q, there are at most two basic elements of S. It turns out that all elements of S are generated from basic elements using primes from these sets.

Theorem 1. *(a) For $n \in S$, the set $\mathcal{P}_{S,n}$ is the set of primes dividing $u_n\Delta$.*

(b) Every element of S can be written in the form $bp_1 \ldots p_r$ for some $r \geq 0$, where $b \in S$ is basic and, for $i = 1, \ldots, r$, the numbers $bp_1 \ldots p_{i-1}$ are also in S, and p_i is in $\mathcal{P}_{S,bp_1\ldots p_{i-1}}$.

(c) The (first kind) basic elements of S are

- 1 *and* 6 *if* $P \equiv 3 \pmod 6$, $Q \equiv \pm 1 \pmod 6$;
- 1 *and* 12 *if* $P \equiv \pm 1 \pmod 6$, $Q \equiv -1 \pmod 6$;
- 1 *only, otherwise.*

Note that the primes in part (b) need not be distinct.

Somer [20, Theorem 4] has many results in the direction of this theorem. In particular, he already noted the importance of 6 and 12 for this problem. Walsh [23, unpublished] gave an equivalent categorization of $S(1, -1)$ (the Fibonacci numbers case), a case where 1 and 12 are the basic elements of $S(1, -1)$.

Note that if α and β are integers, then at least one of P, Q is even, so that 1 is the only basic element in this case. In this case, too, it is known (see André-Jeannin [2]) that $S = \{n : n \mid \alpha^n - \beta^n\}$. (His result is stated assuming that $\gcd(n, \alpha\beta) = 1$, and his proof given for n square-free). This follows straight from Proposition 11 below. Further, for α and β integers with $\gcd(\alpha, \beta) = 1$, Győry [10] proved that, for a fixed integer r, the number of elements of S with r prime factors was finite, and described how to find them. See also [11] for the more general problem of the divisibility of $\alpha^n - \beta^n$ (α, β integers) by powers of n.

Now let $\mathcal{P}_S$ be the set of primes p that divide some n in S. It is easy to see that $\mathcal{P}_S = \cup_{n\in S}\mathcal{P}_{S,n}$. It is interesting to compare $\mathcal{P}_{S,n}$ and $\mathcal{P}_{S,np}$ for n and np in S. Write $u_n = u_n(\alpha, \beta)$ to show the dependence of u_n on α and β, and denote $u_n(\alpha^k, \beta^k)$ by $u_n^{(k)}$. Then since

$$u_{kn} = u_k^{(n)} u_n, \tag{1}$$

we have $u_n \mid u_{np}$, so that $\mathcal{P}_{S,n} \subset \mathcal{P}_{S,np}$ by Theorem 1(b). Thus when we multiply $n \in S$ by a succession of primes according to Theorem 1(b) to stay within S, the associated set $\mathcal{P}_{S,n}$ does not lose any primes. Hence we obtain the following consequence of Theorem 1(a).

Corollary 2. *If $n \in S$ and all prime factors of m divide $u_n\Delta$, then $nm \in S$.*

This is a strengthening of the known result (see e.g., [20, Theorem 5(i)]) that if $n \in S$ and all prime factors of m divide $n\Delta$, then $nm \in S$. In particular ($n = 1$) $\Delta \in S$ and, for $n \in S$, both $u_n = n \cdot (u_n/n) \in S$ and $u_n\Delta \in S$.

In Section 7 we give the conditions on P and Q that make S, $\mathcal{P}_S$, T or $\mathcal{P}_T$ finite. In Section 8 we compare $\mathcal{P}_S$ with the set $\mathcal{P}_{\text{1st}}$ of primes that divide some u_n and the set $\mathcal{P}_T$ with the set $\mathcal{P}_{\text{2nd}}$ of primes that divide some v_n with $n \geq 1$. In Section 9 we briefly discuss divisibility properties of the sequences S and T. These properties are useful for generating the sequences efficiently.

It is of interest to estimate $\{n \in S : n \leq x\}$ and $\{n \in T : n \leq x\}$. It is planned to do this in a forthcoming paper of Shparlinski and the author. For $\mathcal{P}_S$ infinite (and not the set $\mathcal{P}$ of all primes!) it would also be of interest to estimate the relative density of $\mathcal{P}_S$ in $\mathcal{P}$. But this seems to be a more difficult problem (as does the corresponding problem for T).

A basic reference for Lucas numbers is the monograph of Williams [24]. See also Dickson [8, Chapter 17], and Ribenboim [17]. For a more general reference on recurrence sequences see the book [9] by Everest, van der Poorten, Shparlinski, and Ward.

2 Preliminary results for S.

While Theorem 1(b) allows us to multiply $n \in S$ by the primes in $\mathcal{P}_{S,n}$ to stay within S, a vital ingredient in proving Theorem 1(c) is to be able to do the opposite: to divide $n \in S$ by a prime and stay within S. This is provided by the following significant result, due to Somer, generalising special cases due to Jarden [13, Theorem E], Hoggatt and Bergum [12] and Walsh [23] for the Fibonacci sequence (i.e., $P = 1$, $Q = -1$) and André-Jeannin [2] for $\gcd(P, Q) = 1$.

Theorem 3 (Somer [20, Theorem 5(iv)])**.** *Let $n \in S$, $n > 1$, with $p_{\max}$ its largest prime factor. Then, except in the case that P is odd and n is of the form $2^\ell \cdot 3$ for some $\ell \geq 1$, we have $n/p_{\max} \in S$.*

We produce a variant of this result to cover all but two of the exceptional cases, as follows.

Proposition 4. *If P is odd and $n = 2^\ell \cdot 3 \in S$, where $\ell \geq 3$, then $n/2 \in S$.*

The idea of the proof of Theorem 3 is roughly (i.e., ignoring some details) as follows. Let n have prime factorization $n = \prod_p p^{k_p}$, with $\omega(n)$, the *rank of appearance of* n, being the least integer k such that $n \mid u_k$. Then $n \mid u_n$ is equivalent to $\omega(n) \mid n$. Since $\omega(n) = \operatorname{lcm}_p \omega\left(p^{k_p}\right)$, and every $\omega\left(p^{k_p}\right)$ is of the form $p^{k'_p}\ell_p$, where $k'_p < k_p$ and $\ell_p \mid (p^2 - 1)$, it follows that $n \mid u_n$ is equivalent to

$$\operatorname{lcm}_{p|n}\left(p^{k'_p}\ell_p\right) \mid n = \prod_{p|n} p^{k_p}. \tag{2}$$

But since for $p > 2$ all prime factors of $p^2 - 1$ are less than p, and $2^2 - 1 = 3$, if equation (2) holds, it will still hold with n replaced by $n/p_{\max}$ when $p_{\max} > 3$ or $p_{\max} = 3$ and (n odd or $2 \mid n$ with $\ell_2 = 1$). When $p_{\max} = 3$ and $2 \mid n$ with $\ell_2 = 3$, (2) will still hold with n replaced by $n/3$ as long as $n/3$ is divisible by 3.

For the proof of Theorem 1, we first need the following, which dates back to Lucas [15, p. 295] and Carmichael [7, Lemma II]. It is the special case $n = 1$ of Theorem 1(a).

Lemma 5. *For any prime p, p divides u_p if and only if p divides Δ.*

Proof. Now $u_2 = P$ and $\Delta = P^2 - 4Q \equiv u_2 \pmod 2$, so the result is true for $p = 2$. The result is trivial for $\Delta = 0$. Now for $\Delta \neq 0$ and $p \geq 3$,

$$\begin{aligned}\Delta^{(p-1)/2} &= \frac{(\alpha-\beta)^p}{(\alpha-\beta)}\\ &= u_p + \sum_{j=1}^{p-1}\binom{p}{j}\alpha^{p-j}(-\beta)^j/(\alpha-\beta)\\ &= u_p + \sum_{j=1}^{(p-1)/2}\binom{p}{j}(-1)^jQ^ju_{p-2j}\\ &\equiv u_p \pmod p,\end{aligned}$$

giving the result. □

We have the following.

A prime is called *irregular* if it divides Q but not P. Clearly $p \nmid \Delta$ for p irregular. A prime that is not irregular is called *regular*.

Lemma 6 (Lucas [15, pp. 295–297], Carmichael [7, Theorem XII], Somer [20, Proposition 1(viii)], Williams [24, pp. 83–84])**.** *If p is an odd prime with $p \nmid Q$, $p \nmid \Delta$, then $p \mid u_{p-\varepsilon}$, where ε is the Legendre symbol $\left(\frac{\Delta}{p}\right)$. On the other hand, if p is irregular then it does not divide any u_n, $n \geq 1$.*

The following result follows easily from Lemmas 5 and 6.

Corollary 7. *The set $\mathcal{P}_{1\mathrm{st}}$ of primes that divide some u_n, $n \geq 1$ consists precisely of the regular primes.*

Lemma 8 (Somer [20, Theorem 5(ii)])**.** *If $m, n \in S$ then $\operatorname{lcm}(m, n) \in S$.*

Proof. Put $\ell = \operatorname{lcm}(m, n)$. From (1) we have $u_n \mid u_\ell$, $u_m \mid u_\ell$, so $n \mid u_n$, $m \mid u_m$ and hence $\ell \mid u_\ell$. □

Lemma 9. *We have*

(i) If P is odd and $2^\ell \mid u_{12}$, where $\ell \geq 1$, then $2^{\ell-1} \mid u_6$;

(ii) If $3 \mid u_{8k}$ then $3 \mid u_{4k}$.

Proof. Using the notation

$$P^{(k)} = P(\alpha^k, \beta^k) = \alpha^k + \beta^k = v_k, \qquad Q^{(k)} = Q(\alpha^k, \beta^k) = Q^k,$$

we have $P^{(2)} = P^2 - 2Q$ and

$$P^{(4)} = (P^2 - 2Q)^2 - 2Q^2 = P^4 - 4P^2Q + 2Q^2. \tag{3}$$

(i) Take P odd. Then

$$P^{(2)} \equiv \begin{cases} 1 \pmod 4, & \text{if } Q \text{ even;} \\ -1 \pmod 4, & \text{if } Q \text{ odd,} \end{cases}$$

and so $P^{(4)} \equiv P^{(2)} \pmod 4$ and

$$v_6 = P^{(2)}(P^{(4)} - Q^2) \equiv \begin{cases} 1 \pmod 4, & \text{if } Q \text{ even;} \\ 2 \pmod 4, & \text{if } Q \text{ odd.} \end{cases}$$

Since $u_{12} = u_6 v_6$ by (1) and $2 \nmid u_{12}$ for Q even, we get the result.

(ii) Since $u_{4k} = u_k^{(4)} u_4$, it is enough to prove that if $3 \mid u_{2k}^{(4)}$ and $3 \nmid u_4$ then $3 \mid u_k^{(4)}$. Now, working modulo 3, $P^{(4)} \equiv P^2(1 - Q) - Q^2$, using (3) and $P^4 \equiv P^2$. Thus

$$\begin{pmatrix} P^{(4)} \\ Q^{(4)} \end{pmatrix} = \begin{cases} \binom{0}{0}, & \text{if } P \equiv Q \equiv 0; \\ \binom{1}{0}, & \text{if } P \equiv \pm 1, Q \equiv 0; \\ \binom{1}{1}, & \text{if } P \equiv \pm 1, Q \equiv -1; \\ \binom{-1}{1}, & \text{otherwise.} \end{cases}$$

The result holds in the first case because $u_4 \equiv 0$, and in the second case because $u_n^{(4)} \equiv 1$ for all $n \geq 1$. In the other two cases, $u_n^{(4)} \equiv 0$ precisely when $3 \mid n$, so the result holds also in these cases.

□

Proposition 10. *If P is odd and $2^\ell \cdot 3 \in S$, where $\ell \geq 3$, then $2^{\ell-1} \cdot 3 \in S$. In particular, then $12 \in S$.*

Proof. Take P odd. Then $P^{(2)} = P^2 - 2Q$ is also odd, and hence so are all $P^{(2^\ell)} = v_{2^\ell}$ for $\ell \geq 0$. Then for $\ell \geq 3$, using (1) and $u_{2k} = u_k v_k$ we have

$$u_{2^\ell . 3} = u_{12}^{(2^{\ell-2})} u_{2^{\ell-2}} = u_{12}^{(2^{\ell-2})} v_{2^{\ell-3}} v_{2^{\ell-4}} \dots v_2 v_1.$$

So if $2^\ell \mid u_{2^\ell . 3}$ then $2^\ell \mid u_{12}^{(2^{\ell-2})}$ so, by Lemma 9(i), $2^{\ell-1} \mid u_6^{(2^{\ell-2})}$. Hence

$$2^{\ell-1} \mid u_6^{(2^{\ell-2})} u_{2^{\ell-2}} = u_{2^{\ell-1} . 3}.$$

Also, if $3 \mid u_{2^\ell . 3}$ where $\ell \geq 3$ then $3 \mid u_{2^{\ell-1} . 3}$, by Lemma 9(ii). Thus we have proved that if $\ell \geq 3$ and $2^\ell \cdot 3 \in S$ then $2^{\ell-1} \cdot 3 \in S$. Then $12 \in S$ follows. □

Proposition 11. *For any positive integer n and distinct integers a, b,*

$$n \mid a^n - b^n \Longrightarrow n \mid \frac{a^n - b^n}{a - b}.$$

Proof. For any prime p, suppose that $p^\ell \| a - b$ and $p^r \| n$. It is clearly enough to prove that $p^{r+\ell} \mid a^n - b^n$ whenever $\ell > 0$. Put $a = b + \lambda p^\ell$. Then

$$\begin{aligned} a^n - b^n &= \sum_{k=1}^{n} \binom{n}{k} \lambda^k p^{\ell k} b^{n-k} \\ &= \sum_{k=1}^{n} \frac{n}{k} \binom{n-1}{k-1} \lambda^k p^{\ell k} b^{n-k} \\ &\equiv 0 \pmod{p^L}, \end{aligned}$$

where

$$\begin{aligned} L &\geq r + \min_{k=1}^{n} (\ell k - \lfloor \log_p k \rfloor) \\ &\geq r + \ell + \min_{k=1}^{n} (\ell(k-1) - \log_2 k) \\ &\geq r + \ell + \min_{k=1}^{n} ((k-1) - \log_2 k) \\ &= r + \ell. \end{aligned}$$

□

3 Proof of Theorem 1.

To prove part (a), take $n \in S$ and p prime. First note that, from (1), $u_{np} = u_p^{(n)} u_n$. Now suppose that $np \mid u_{np}$. Then either $p \mid u_n$, or, by Lemma 5, we have $p \mid \Delta^{(n)}$, where $\Delta^{(n)} = (\alpha^n - \beta^n)^2 = u_n^2 \Delta$. Hence $p \mid u_n \Delta$.

Conversely, suppose $p \mid u_n \Delta$. Then $p \mid \Delta^{(n)}$, so that, by Lemma 5, $p \mid u_p^{(n)}$, giving $pn \mid u_p^{(n)} u_n = u_{np}$.

To prove (b), take $n \in S$, $n \neq 1, 6$ or 12. If $3 \in S$ then $3/3 = 1 \in S$. Otherwise, by Theorem 3 and Proposition 10, we have $n/p \in S$ for some prime factor p of n. Thus we obtain a sequence $n, n/p, (n/p)/p', \ldots$ of elements of S, which stops only at 1, 6 or 12. But clearly 6 and 12 cannot both be basic, so the process will stop at either 1 (always basic!) or at most one of 6 and 12. This shows that this sequence, written backwards, must be of the form $b, bp_1, bp_1p_2, \ldots, bp_1 \ldots p_r$, say, as required. By (a), we know that p_i is in $\mathcal{P}_{S, bp_1 \ldots p_{i-1}}$.

To prove (c), we just need to find for which P, Q the numbers 6 or 12 are basic.

The case $\boldsymbol{6 \in S, 3 \notin S, 2 \notin S}$. Since $u_2 = P$, we know that $2 \in S$ iff P is even. Hence P is odd. Also

$$u_6 = u_3 v_3 = (P^2 - Q)(P^2 - 3Q)P. \tag{4}$$

As $6 \mid u_6$ and $3 \nmid u_3 = P^2 - Q$, we have $3 \mid P$, and so $Q \equiv \pm 1 \pmod 3$. Also Q must be odd, so $P \equiv 3 \pmod 6$ and $Q \equiv \pm 1 \pmod 6$.

The case $12 \in S, 6 \notin S, 4 \notin S$. Since $2 \notin S$ by Corollary 2, we have P odd, as above. Now $u_{12} = u_6 v_6$ and

$$v_6 = v_3^{(2)} = (P^2 - 2Q)((P^2 - 2Q)^2 - 3Q^2). \tag{5}$$

If Q were even, then by (4) and (5) u_6, v_6, and u_{12} would all be odd. So Q is odd. As u_6 is then even, $3 \nmid u_6$, and we have $P \equiv \pm 1 \pmod 3$ and $Q \equiv 0$ or $-1 \pmod 3$. As $3 \mid u_{12}$, also $3 \mid v_6 \equiv (P^2 - 2Q)^3 \pmod 3$, giving $Q \equiv -1 \pmod 3$. Hence $P \equiv \pm 1 \pmod 6$ and $Q \equiv -1 \pmod 6$.

The converse for both of these cases is easily checked.

4 The set T

The results for the set $T = \{n \in \mathbb{N} : n \mid v_n\}$ differ slightly from those for S. Essentially, this is because of difficulties at the prime 2: v_n divides v_{np} for p odd, but not in general for $p = 2$. The main result is the following. For $n \in T$, define $\mathcal{P}_{T,n}$ to be the set of primes p such that $np \in T$. A prime is said to be *special* if it divides both P and Q. It is clear from applying the recurrence relation that all v_n for $n \geq 1$ are divisible by $\gcd(P, Q)$, and so by all special primes. We say that an element n of T is *(second kind) basic* if there is no prime p such that n/p is in T.

Theorem 12. *(a) For $n \in T$, the set $\mathcal{P}_{T,n}$ is the set of odd primes dividing v_n, with the possible inclusion of 2. Specifically, the prime 2 is in $\mathcal{P}_{T,n}$ if and only if n is a product of special primes and either*

- *P is even;*

  or

- *Q is odd and $3 \mid n$.*

(b) Every element of T can be written in the form $bp_1 \dots p_r$ for some $r \geq 0$, where $b \in T$ is (second kind) basic and, for $i = 1, \dots, r$, the numbers $bp_1 \dots p_{i-1}$ are also in T, and p_i is in $\mathcal{P}_{bp_1 \dots p_{i-1}}$.

(c) The (second kind) basic elements of T are

- *1 and 6 if $P \equiv \pm 1 \pmod 6$, $Q \equiv -1 \pmod 6$;*
- *1 only, otherwise.*

As in Theorem 1, the primes in part (b) of Theorem 12 need not be distinct. Note that parts (a) and (b) of the theorem imply that, unless 2 is special, no element of T is divisible by 4. Again, Somer [21, Theorem 4] had many results concerning the set T. In particular, he already noted the importance of 6 for its structure.

We now compare $\mathcal{P}_{T,n}$ and $\mathcal{P}_{T,np}$, as we did $\mathcal{P}_{S,n}$ and $\mathcal{P}_{S,np}$. But, in this case, the prime 2 is, unsurprisingly, anomalous.

Corollary 13. *(a) For an odd prime p in $\mathcal{P}_{T,n}$, we have $p \in \mathcal{P}_{T,np}$;*

(b) For q an odd prime with $q \in \mathcal{P}_{T,n}$, we have $q \in \mathcal{P}_{T,2n}$ if and only if $q \mid Q$;

(c) For $2 \in \mathcal{P}_{T,n}$, we have $2 \in \mathcal{P}_{T,2n}$ if and only if 2 is special.

Proof. Part (a) follows from the fact that for p odd $v_n \mid v_{np}$, combined with Theorem 12(a). For (b), we know from Theorem 12(a) that $q \mid v_n$. Then from $v_{2n} = v_n^2 - 2Q^n$ we see that $q \mid v_{2n}$ iff $q \mid Q$. For (c), we know from Theorem 12(a) that for $2 \in \mathcal{P}_{T,2n}$ all prime divisors of $2n$ are special, so 2 is special. Conversely, if 2 is special, then all prime factors of $2n$ are special, and P is even, so that, by Theorem 12(a), $2 \in \mathcal{P}_{T,2n}$. □

Corollary 14. *If $n \in T$ and*

- *all odd prime factors of m divide v_n;*

  and

- *if m is even then every prime divisor of nm is special;*

then $nm \in T$.

Proof. On successively multiplying n by first the odd and then the even prime divisors of m, we see from Theorem 12(a) that the stated conditions ensure that we stay within T while doing this. □

This result extends Theorem 5(i) of Somer [21], which has the condition that 'm is a product of special primes or divides n' instead of 'all odd prime factors of m divide v_n'.

5 Preliminary results for T.

We first quote the important result of Somer for T, corresponding to his result (Theorem 3 above) for S.

Theorem 15 (Somer [21, Theorem 5])**.** *Theorem 3 holds with the set S replaced by the set T.*

Jarden [13, Theorem E] proved this result for the classical Lucas sequence (i.e., $P = 1$, $Q = -1$) under the restriction $p_{\max} \neq 3$.

Lemma 16. *Suppose q is a special prime. Then $q^{e_n} \mid v_n$, where $e_n \geq \lfloor \log_q n \rfloor$.*

Proof. From the recurrence, it is easy to see that we can take

$$e_n = \begin{cases} \left\lfloor \frac{n}{2} \right\rfloor + 1, & \text{if } q = 2; \\ \left\lfloor \frac{n+1}{2} \right\rfloor, & \text{if } q \geq 3, \end{cases}$$

the slightly higher value for $q = 2$ coming from the fact that $v_0 = 2$. Then use $\lfloor \log_q n \rfloor \leq \left\lfloor \frac{n+1}{2} \right\rfloor$. □

We then immediately obtain the following.

Corollary 17 (Special case of Somer [21, Theorem 5(i)])**.** *If n is a product of special primes then it belongs to T.*

We can now extend Theorem 15 as follows.

Proposition 18. *If $\ell \geq 2$ and $2^\ell \cdot 3 \in T$, then $2^\ell \in T$.*

Proof. Put $L = 2^\ell$. If 2 is special, then, by Corollary 17, $L \in T$ for all $\ell \geq 1$. So we can assume that 2 is not special. We then know that Q must be odd, as if it were even then we would have $2 \mid v_{3L}$ and $v_{3L} \equiv P^{3L} \pmod{Q}$, so P would be even and 2 special.

From $L \mid v_{3L} = v_L(v_L^2 - 3Q^L)$ we see that if v_L were odd then, as L is even, Q^L is a square, and so $v_L^2 - 3Q^L \equiv 2 \pmod{4}$, giving $2^1 \| v_{3L}$, a contradiction. Hence v_L is even, and $L \mid v_L$. □

Next, we consider the set $\mathcal{P}_T$ of primes that divide some $n \in T$. To set our result in context, recall that $\mathcal{P}_{\mathrm{2nd}}$ denotes the set of the primes dividing v_n for some $n \geq 1$. Clearly $\mathcal{P}_T$ is a subset of $\mathcal{P}_{\mathrm{2nd}}$. Our next result, essentially dating back to Lucas [15], describes this set. See also Somer [21, Proposition 2(iv)].

Proposition 19. *The set $\mathcal{P}_{\mathrm{2nd}}$ is a proper subset of $\mathcal{P}_{\mathrm{1st}}$. It consists of*

- *the primes p for which the rank of appearance $\omega(p)$ of p (in (u_n)) is even;*
- *the special primes;*
- *the prime 2, unless P is odd and Q is even.*

Proof. Take a prime p with $p \nmid 2Q$, and let $\omega = \omega(p)$. If ω is even, then the identity $u_{2n} = u_n v_n$ for $n = \omega/2$ shows that $p \mid v_n$, $p \in \mathcal{P}_{\mathrm{2nd}}$. The identity also shows that $\mathcal{P}_{\mathrm{2nd}} \subset \mathcal{P}_{\mathrm{1st}}$.

Conversely, if $p \in \mathcal{P}_{\mathrm{2nd}}$, say $p \mid v_n$, then $p \mid u_{2n}$, so that, by [20, Proposition 1(iv)], $\omega \mid 2n$. However, from the identity

$$u_n^2 - \Delta v_n^2 = 4Q^n, \tag{6}$$

we have $p \nmid u_n$, so that ω is even.

Now take a prime p with $p \mid Q$. Then from $v_n \equiv P^n \pmod{p}$ we see that, for p to be in $\mathcal{P}_{\mathrm{2nd}}$, p must be special. In particular, $2 \notin \mathcal{P}_{\mathrm{2nd}}$ when P is odd and Q is even. Further, if P is even then $v_1 = P$ is even, while if P and Q are both odd then $v_3 = P(P^2 - 3Q)$ is even.

Finally, for $p \nmid 2Q$, choose m odd, and sufficiently large that we can take p to be a primitive prime divisor of u_m. Then we have $\omega(p) = m$, and hence $p \in \mathcal{P}_{\mathrm{1st}} \setminus \mathcal{P}_{\mathrm{2nd}}$.

□

Our next lemma is an easy exercise. Dickson [8, pp. 67 and 271] traces the result back to an 'anonymous writer' in 1830 [25], and also to Lucas [15, p. 229].

Lemma 20. *For p an odd prime and $j = 1, 2, \ldots, (p-1)/2$, the expression $B_j := \binom{p-1}{j} - (-1)^j$ is divisible by p.*

The following result essentially dates back to Lucas [15, p. 210] and Carmichael [6, Theorem X].

Lemma 21. *(i) For $n \in \mathbb{N}$ and any prime p, p divides v_{np} if and only if p divides v_n.*

(ii) For $n \in \mathbb{N}$ and any odd prime p, v_n divides v_{np} and $v_{np}/v_n \equiv v_n^{p-1} \pmod{p}$.

Proof. (i) Now $v_2 = v_1^2 - 2Q$, which is even iff v_1 is even. Also, for $p \geq 3$,

$$v_1^p = (\alpha+\beta)^p = v_p + \sum_{j=1}^{(p-1)/2} \binom{p}{j} Q^j v_{p-2j} \equiv v_p \pmod{p}. \tag{7}$$

Now replace α, β by α^n, β^n.

(ii) Taking p odd and B_j defined as in Lemma 20, we have

$$\begin{aligned} v_p &= (\alpha+\beta)(\alpha^{p-1} - \alpha^{p-2}\beta + \cdots + \beta^{p-1}) \\ &= (\alpha+\beta)((\alpha+\beta)^{p-1} - \sum_{j=1}^{p-2} B_j \alpha^{p-1-j}\beta^j) \\ &= v_1 \left(v_1^{p-1} - \sum_{j=1}^{(p-3)/2} B_j Q^j v_{p-1-2j} - B_{(p-1)/2} Q^{(p-1)/2} \right). \end{aligned}$$

so that the result of p odd follows by replacing α, β by α^n, β^n and using Lemma 20. $\square$

6 Proof of Theorem 12

We now prove part (a) of Theorem 12. First take p odd and $n \in T$. Then, by Lemma 21(i), if $p \nmid v_n$ then $p \nmid v_{np}$, so $np \notin T$. Conversely, if $p^\lambda \| v_n$ for some $\lambda \geq 1$ then by Lemma 21(ii) $p^{\lambda+1} \mid v_{np}$. Since $n \mid v_n$ and $pv_n \mid v_{np}$ we have $np \in T$.

Now take $p = 2$, and suppose that both n and $2n$ are in T. First note that v_n must be even, as otherwise $v_{2n} = v_n^2 - 2Q^n$ would be odd. Also, we have $n \mid Q^n$, so that every prime factor q of n divides Q. (Note that this works too if $q = 2$, as then $4 \mid v_{2n}$.) But q must also divide P, as otherwise $v_n \equiv P^n \not\equiv 0 \pmod{q}$. Hence q is special, and n is a product of special primes. If n is even, then 2 is special, so P and Q are both even. If n is odd then, because v_n is even, we must have either P even and Q odd or (from the recurrence) P and Q both odd and $3 \mid n$. So we have either P even or Q odd and $3 \mid n$.

Conversely, assume that $n \in T$ is a product of special primes, and either P is even or (Q is odd and $3 \mid n$). We know from Corollary 17 that every product of special primes is in T. So if 2 is special, then $2n \in T$. So we can assume 2 is not special, and hence that n is odd. If P is even, then, from the recurrence, all the v_k, in particular v_n and v_{2n}, are even. Also, if P and Q are both odd and $3 \mid n$, then v_n and $v_{2n} = v_n^2 - 2Q^n$ are both even. Since for every prime factor q of n with $q^\lambda \| n$ we have $\lambda \leq \log_q n < n$, so that $n \mid Q^n$. Hence $2n \mid v_{2n}$, $2n \in T$.

The proof of part (b) is just the same as that for Theorem 1(b).

To prove part (c): we see easily from Theorem 15 and Proposition 18 that the only possible (second kind) basic numbers are 1 and 6. To find the conditions on P and Q that make 6 basic, we assume that $6 \in T$ but $2 \notin T$, $3 \notin T$. Then $v_2 = P^2 - 2Q$ is odd, so P is odd. Also $3 \nmid v_3 = P(P^2 - 3Q)$, so $P \equiv \pm 1 \pmod 6$. From $6 \mid v_6 = v_2(v_2^2 - 3Q^2)$ we have Q odd and $3 \mid v_2 \equiv 1 - 2Q \pmod 3$, so that $Q \equiv -1 \pmod 6$. Conversely, if $P \equiv \pm 1 \pmod 6$ and $Q \equiv -1 \pmod 6$ then it is easily checked that 6 is basic. This proves part (c).

7 Finiteness results for S and for T.

In this section we look at when S, $\mathcal{P}_S$, and T, $\mathcal{P}_T$ are finite. The results given here are essentially reformulations of results of Somer [20], [21].

Theorem 22. *The set S is finite if and only if $\Delta = 1$, in which case $S = \{1\}$. For S infinite, $\mathcal{P}_S$ is finite when $Q = 0$ and $P \neq 0$, in which case $\mathcal{P}_S$ consists of the prime divisors of P. Otherwise, $\mathcal{P}_S$ is also infinite. Furthermore, $\mathcal{P}_S$ is the set $\mathcal{P}$ of all primes if and only if every prime divisor of Q is special. (This includes the case $Q = \pm 1$.)*

For the proof, we note first that when $\Delta = 1$, α and β are consecutive integers, and 1 is the only basic element. But there are no primes p dividing $u_1\Delta = 1$, so $\mathcal{P}_{S,1}$ is empty, and $S = \{1\}$. In all other cases, $|u_1\Delta| > 1$, $\mathcal{P}_{S,1}$ is nonempty, with $p \in \mathcal{P}_{S,1}$ say, and then, by Corollary 2, $p^k \in S$ for all $k \geq 0$, making S infinite.

Now assume S is infinite. We recall that $(u_n)_{n\geq 0}$ is called *degenerate* if $Q = 0$ or α/β is a root of unity. (The latter alternative includes the case $P = 0$, $Q \neq 0$.) We consider the two cases of (u_n) being degenerate or nondegenerate separately. If (u_n) is degenerate, then by [20, Theorem 9] either

- $P \neq 0$ and $Q = 0$, so that then S consists of those n whose prime factors all divide P, and $\mathcal{P}_S = \mathcal{P}_{1\text{st}}$ is the set of prime divisors of P;

  or

- for some $r = 1, 2, 3, 4$ or 6, S has a subset $\{rk : k \in \mathbb{N}\}$ where $u_{rk} = 0$, so that $\mathcal{P}_S = \mathcal{P}_{1\text{st}} = \mathcal{P}$.

Now consider the case of (u_n) nondegenerate. Then, by Somer [20, Theorem 1], all but finitely many u_n have a primitive prime divisor (a prime dividing u_n that do not divide u_m for any $m < n$). So, using Theorem 1(a), $\mathcal{P}_S$ is infinite. Somer's theorem is based on results of Lekkerkerker [14] and Schinzel [18]. In fact Bilu, Hanrot and Voutier [5] have proved that for such sequences with no special primes every u_n with $n > 30$ has a primitive divisor. They also listed exceptions with $n \leq 30$. Hence u_{p^k} has a primitive prime divisor for all sufficiently large k, making $\mathcal{P}_S$ infinite. See Abouzaid [1] for corrections to their list. Also Stewart [22] and Shorey and Stewart [19] gave lower bounds for the largest prime divisor of u_n.

This proof will be complete after we have proved the following. While this result is contained in Somer [20, Theorem 8], we give another proof here.

Proposition 23. *The set $\mathcal{P}_S$ is the whole of $\mathcal{P}$ if and only if all primes are regular.*

Proof. First note that if there are any irregular primes then, by Corollary 7, $\mathcal{P}_S$, being a subset of $\mathcal{P}_{1\text{st}}$, cannot be the whole of $\mathcal{P}$.

Conversely, assume all primes are regular, so that any prime factor p of Q also divides P. Note that then $p \mid \Delta$. To show that all primes belong to $\mathcal{P}_S$, we proceed by induction. We first show that $2 \in \mathcal{P}_S$. If $u_2 = P$ is even, then $2 \in S$, $2 \in \mathcal{P}_S$. So we can take P odd. Then Q must be odd, too, by our assumption. Then $u_3 = P^2 - Q$ is even, and hence so is $u_6 = u_3 v_3$. We claim that either $3 \mid u_6$, in which case $6 \in S$, $2, 3 \in \mathcal{P}_S$, or $12 \in S$, with the same implication.

- If $P \equiv 3 \pmod 6$, $Q \equiv 3 \pmod 6$, then $3 \mid u_n$ for all $n \geq 2$, so that $3 \mid u_6$.
- If $P \equiv 3 \pmod 6$, $Q \equiv \pm 1 \pmod 6$, then 6 is basic, by Theorem 1(c).
- If $P \equiv \pm 1 \pmod 6$, $Q \equiv -1 \pmod 6$, then 12 is basic, by Theorem 1(c).
- If $P \equiv \pm 1 \pmod 6$, $Q \equiv 1 \pmod 6$, then $3 \mid u_3$ and so $3 \mid u_3 v_3 = u_6$.

Hence $2 \in \mathcal{P}_S$, as claimed.

We now assume that $q \in \mathcal{P}_S$ for every prime $q < p$, where p is a prime at least 3. We have just shown that this is true for $p = 3$. By Lemma 8, we know that for any exponents $\varepsilon_q = 0$ or 1 there is a positive integer k such that $k \prod_{q<p} q^{\varepsilon_q} \in S$; hence, by Corollary 2, $k \prod_{q<p} q^{e_q} \in S$ for any exponents $e_q \geq \varepsilon_q$.

By Lemma 6, $p \mid u_{p+\varepsilon}$, for some $\varepsilon = \pm 1$. As $p > 2$, all prime factors of $p + \varepsilon$ are less than p so, by the induction hypothesis, $k(p + \varepsilon) \in S$ for some k. If $p \mid k$ then $p \in \mathcal{P}_S$. If $p \nmid k$ then, using (1), we have

$$u_{pk(p+\varepsilon)} = u_p^{(k(p+\varepsilon))} u_{k(p+\varepsilon)} = u_{pk}^{(p+\varepsilon)} u_{p+\varepsilon},$$

so that $pk(p + \varepsilon) \in S$, $p \in \mathcal{P}_S$. This proves the induction step. $\square$

This completes the proof of Theorem 22.

We now consider the finiteness (or otherwise) of T and $\mathcal{P}_T$.

Theorem 24 (Somer [21, Theorems 8 and 9]). *The set T is finite in the following two cases:*

- $P = \pm 1$, $Q \not\equiv -1 \pmod 6$, *in which case* $T = \{1\}$*;*
- $P = \varepsilon_1 2^k$, $Q = 2^{2k-1} + \varepsilon_2$, *where k is a positive integer, and* $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, *in which case* $T = \{1, 2\}$.

Otherwise, T is infinite. For T infinite, $\mathcal{P}_T$ is finite precisely when P, Q are not both 0 and either

- $P^2 = Q$, *in which case $\mathcal{P}_T$ is the set of prime divisors of* $2P$

  or

- $P^2 = 4Q$ *or* $Q = 0$, *in which case $\mathcal{P}_T$ is the set of prime divisors of* P.

Otherwise, for T infinite, $\mathcal{P}_T$ is also infinite.

Proof. If T contains an integer n having an odd prime factor p then, by Theorem 12(a), $p^k n \in T$ for all $k \geq 0$. In particular, if $P = \pm 1$ and $Q \equiv -1 \pmod 6$, then $6 \in T$, so that T is infinite. On the other hand, if $P = \pm 1$ and $Q \not\equiv -1 \pmod 6$, then 1 is the only basic element of T, and $v_1 = P$ has no prime factors so that, by Theorem 12(a), $\mathcal{P}_{T,1}$ is empty, and hence $T = \{1\}$.

Again starting with $1 \in T$, we see that T is infinite if P has any odd prime factors. Also, T is infinite if P is $\pm$ a positive power of 2 and 2 is special, as then $2^k \in T$ for all $k \geq 0$, by Theorem 12(a).

It therefore remains only to consider the case of $P = \pm 2^k$, $k \geq 1$ and Q odd, so that 2 is not special. Then $2 \in T$ and $4 \notin T$, by Theorem 12(a). If v_2 has an odd prime factor p, then $2p^k \in T$ for all $k \geq 0$, so that T is again infinite. Finally, if v_2 is $\pm$ a power of 2, then $T = \{1, 2\}$. This happens only when $v_2 = 2^{2k} - 2Q = \pm 2$, so that $Q = 2^{2k-1} \mp 1$, as claimed.

Now take T infinite, with P, Q not both 0. If the sequence (v_n) is degenerate, then, using Somer [21, Theorem 9], we get either $P^2 = Q$, $P^2 = 4Q$ or $Q = 0$, and $\mathcal{P}_T$ being the set of prime divisors of P, as required. On the other hand, if (v_n) is not degenerate then by Somer [21, Theorem 1] for sufficiently large n every v_n has a primitive prime divisor. Hence we can find an infinite sequence of numbers n in T such that np is again in T, where p is a primitive prime divisor of v_n. (Here we are using Theorem 12(a).) Thus $\mathcal{P}_T$ then contains infinitely many primes p. □

8 The sets $\mathcal{P}_S$ and $\mathcal{P}_T$.

From the proof of Theorem 22 we see that $\mathcal{P}_S = \mathcal{P}_{\text{1st}}$ for (u_n) degenerate or all primes being regular. Our next result takes care of the remaining cases. I thank Larry Somer and the referee for pointing out how the proof of this could be completed.

Proposition 25. *If (u_n) is nondegenerate and there are irregular primes, then $\mathcal{P}_S$ is a proper subset of $\mathcal{P}_{\text{1st}}$.*

Proof. Take (u_n) nondegenerate and having an irregular prime f. Then, from the discussion preceding Proposition 23, every u_n for n sufficiently large has a primitive prime divisor. Indeed, if $\gcd(P, Q) = 1$ this is true for $n > 30$. Hence for ℓ sufficiently large, $u_{\ell f}$ has a primitive prime divisor, p say, so that $\omega(p) = \ell f$.

Then if, for some k, kp were in S, we would have $kp \mid u_{kp}$, so that, by [20, Proposition 1(iv)], $\omega(p)$, and hence f, would divide kp. Hence f would divide u_n, contradicting Corollary 7. Thus $p \notin \mathcal{P}_S$. □

We have in fact shown that no prime whose rank of appearance is a multiple of any irregular prime f will belong to $\mathcal{P}_S$. The referee has remarked that, when α/β is rational, the density of such primes has been precisely computed in many cases. For $f > 2$ and α/β not an f-th power, it is $f/(f^2 - 1)$. See Ballot [4, Theorem 3.2.3] and also Moree [16].

Using a similar method, we can also prove the corresponding result for T.

Proposition 26. *The set $\mathcal{P}_T$ is a proper subset of $\mathcal{P}_{\text{2nd}}$.*

Proof. Let f be a primitive prime divisor of u_n for some odd n with $f \nmid 2Q$. Then, by Proposition 19, $f \in \mathcal{P}_{1\text{st}} \setminus \mathcal{P}_{2\text{nd}}$. Now, taking ℓ sufficiently large, let p be a primitive prime divisor of $u_{2\ell f}$. Then, as $u_{2\ell f} = u_{\ell f} v_{\ell f}$, $p \mid v_{\ell f}$. Suppose $p \in \mathcal{P}_T$, so that, for some k, $kp \in T$, and hence $kp \mid v_{kp}$. But then by Somer [21, Proposition 2(vii)], kp is a multiple of ℓf. In particular, $f \mid v_{kp}$, contradicting $f \notin \mathcal{P}_{2\text{nd}}$. So $p \notin \mathcal{P}_T$. □

9 Divisibility properties of S and of T.

From Theorem 1 we can consider S as a graph spanned by a forest of one or two trees, with each node corresponding to an element of S, and the root nodes of the trees being $\{1\}$, $\{1, 6\}$ or $\{1, 12\}$. Each edge can be labelled p; it rises from a node $n \in S$ to a node $np \in S$, where p is some prime divisor of $u_n\Delta$. One spanning forest is obtained by taking only the edges $n \to np$, where p is the largest prime factor of np such that $n \in S$. (By Theorem 3 and Proposition 4, p is either $p_{\max}$ or 2). Thus every node above n in the tree is divisible by n. Next, call a *cutset* of the forest a set C of nodes with the property that every path from a root to infinity must contain some vertex of the cutset. Then we clearly have the following.

Proposition 27. *For a cutset C of S, every element of S either lies below C, or it is divisible by some node of C.*

Judicious choice of a cutset places severe divisibility restrictions on elements of S, and so, using this, one can search for elements of S up to a given bound very efficiently.

The same argument applies equally to T, using Theorem 12, with p being either an odd prime divisor of v_n or, under the conditions described in that theorem, the prime 2. For instance, applying this idea to the sequence T of example 2 below, every element of that sequence except 1, 3, 9, 27 and 81 is divisible either by 171 or 243 or 13203 or 2354697 or 10970073 or 22032887841. See [3] for details.

10 Examples

1. $P = 1, Q = -1$ (the classical Fibonacci and Lucas numbers.) Here $\Delta = 5$,

$$S = 1, 5, 12, 24, 25, 36, 48, 60, 72, 96, 108, 120, 125, 144, 168, 180, \ldots,$$

with 1 and 12 basic (A023172 in Neil Sloane's *Encyclopedia*), while $\mathcal{P}_S$ is the whole of $\mathcal{P}$ (see Theorem 22),

$$T = 1, 6, 18, 54, 162, 486, 1458, 1926, 4374, 5778, 13122, 17334, \ldots,$$

with 1 and 6 basic (A016089), and

$$\mathcal{P}_{2\text{nd}} = 2, 3, 7, 11, 19, 23, 29, 31, 41, 43, 47, 59, 67, 71, 79, 83, 101, 103, 107, 127, \ldots,$$

(A140409) of which $\mathcal{P}_T$ is a subsequence:

$$\mathcal{P}_T = 2, 3, 107, 1283, 8747, 21401, 34667, 46187, \ldots,$$

(A129729).

2. $P = 3, Q = 2$, where $u_n = 2^n - 1$, $v_n = 2^n + 1$. Here $S = \{1\}$ as $\Delta = 1$, and

$$T = 1, 3, 9, 27, 81, 171, 243, 513, 729, 1539, 2187, 3249, \ldots,$$

with 1 basic (A006521). Also

$$\mathcal{P}_{\text{2nd}} = 3, 5, 11, 13, 17, 19, 29, 37, 41, 43, 53, 59, 61, 67, 83, 97, 101, 107, 109, \ldots,$$

(A014662 – see also A091317), of which

$$\mathcal{P}_T = 3, 19, 163, 571, 1459, 8803, 9137, 17497, 41113, \ldots$$

(A057719) is a subsequence. Note too that, by Proposition 11 and the fact that all $n \in T$ are odd, we have $T = S(-1, -2)$. Also $S = T(-1, -2) = \{1\}$.

3. $P = 3$, $Q = 5$, $\Delta = -11$,

$$S = 1, 6, 11, 12, 18, 24, 36, 48, 54, 66, 72, 96, 108, 121, 132, 144, 162, 168, 192, 198, \ldots$$

with 1 and 6 basic, with $\mathcal{P}_{\text{1st}}$ consisting of all primes except the irregular prime 5, and

$$\mathcal{P}_S = 2, 3, 7, 11, 13, 17, 23, 37, 41, 43, 67, 71, 73, 83, 89, 97, 101, 103, 107, 113, \ldots.$$

Also

$$T = 1, 3, 9, 27, 81, 153, 243, 459, 729, 1377, 2187, 2601, 4131, 4401, 6561, 7803, \ldots$$

with only 1 basic,

$$\mathcal{P}_{\text{2nd}} = 2, 3, 7, 13, 17, 19, 23, 37, 43, 47, 53, 67, 73, 79, 83, 97, 103, 107, 113, \ldots$$

and

$$\mathcal{P}_T = 2, 3, 17, 103, 163, 373, 487, 1733, \ldots.$$

11 Additional remarks.

1. It would be interesting to see whether the analysis of the paper could be extended to other second-order recurrence sequences, or indeed to any recurrences of higher order.

2. In [3], what we called 'primitive' solutions of $n \mid 2^n + 1$ should in fact have been called *fundamental* solutions, following Jarden [13, p. 70] and Somer [20, p. 522], [21, p. 482]. However, this definition has been superseded by the notion of a basic element (of S or of T) as in this paper.

3. In example 1 of Section 10 above we have 24 and $25 \in S = S(1, -1)$. Are these the only consecutive integers in $S(1, -1)$?

12 Acknowledgements

I am very grateful to both Larry Somer and the referee for their detailed contructive comments on an earlier version of this paper. Also, I thank Joe Silverman for a helpful comment.

References

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

[2] Richard André-Jeannin, Divisibility of generalized Fibonacci and Lucas numbers by their subscripts, *Fibonacci Quart.* **29** (1991), 364–366.

[3] Toby Bailey and Chris Smyth, Primitive solutions of $n \mid 2^n + 1$, 2pp., linked from `http://www.research.att.com/~njas/sequences/A006521`, 2008.

[4] Christian Ballot, Density of prime divisors of linear recurrences, *Mem. Amer. Math. Soc.* **115** (1995), no. 551, 102pp.

[5] Yu. Bilu, G. Hanrot, and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), 75–122.

[6] R. D. Carmichael, Note on a recent problem in the American Mathematical Monthly, *Amer. Math. Monthly* **14** (1907), 8–9.

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

[8] Leonard Eugene Dickson, *History of the Theory of Numbers. Vol. I: Divisibility and primality.*, Chelsea Publishing Co., New York, 1966.

[9] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003.

[10] Kálmán Győry, Az $a^n \pm b^n$ alakú számok osztóiról két számelméleti feladat kapcsán [On divisors of numbers of the form $a^n \pm b^n$], *Középiskolai Matematikai Lapok* [Mathematical Journal for Secondary Schools] **41** (1991), 193–201.

[11] Kálmán Győry and Chris Smyth, The divisibility of $a^n - b^n$ by powers of n, to appear.

[12] Verner E. Hoggatt, Jr. and Gerald E. Bergum, Divisibility and congruence relations, *Fibonacci Quart.* **12** (1974), 189–195.

[13] Dov Jarden, Divisibility of Fibonacci and Lucas numbers by their subscripts, *Recurring Sequences: A Collection of Papers*, Second edition. Revised and enlarged, Riveon Lematematika, Jerusalem (Israel), 1966, pp. 68–75.

[14] C. G. Lekkerkerker, Prime factors of the elements of certain sequences of integers. I, II, *Nederl. Akad. Wetensch. Proc. Ser. A.* **56** = *Indagationes Math.* **15** (1953), 265–276, 277–280.

[15] Edouard Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–196, 197–240, 289–321.

[16] Pieter Moree, On primes p for which d divides $\mathrm{ord}_p(g)$, *Funct. Approx. Comment. Math.* **33** (2005), 85–95.

[17] Paulo Ribenboim, The Fibonacci numbers and the Arctic Ocean, *Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics* (Munich, 1993), Sympos. Gaussiana, de Gruyter, Berlin, 1995, pp. 41–83.

[18] Andrzej Schinzel, The intrinsic divisors of Lehmer numbers in the case of negative discriminant, *Ark. Mat.* **4** (1962), 413–416 (1962).

[19] T. N. Shorey and C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. II, *J. London Math. Soc.* (2) **23** (1981), 17–23.

[20] Lawrence Somer, Divisibility of terms in Lucas sequences by their subscripts, *Applications of Fibonacci numbers*, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 515–525.

[21] Lawrence Somer, Divisibility of terms in Lucas sequences of the second kind by their subscripts, *Applications of Fibonacci numbers*, Vol. 6 (Pullman, WA, 1994), Kluwer Acad. Publ., Dordrecht, 1996, pp. 473–486.

[22] C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers, *Proc. London Math. Soc.* (3) **35** (1977), 425–447.

[23] Gary Walsh, On integers n with the property $n \mid f_n$, 5pp., unpublished, 1986.

[24] Hugh C. Williams, *Édouard Lucas and Primality Testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, 22, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication.

[25] Anonymous Writer, Théorèmes et problèmes sur les nombres, *J. Reine Angew. Math.* **6** (1830), 100–106.

2000 *Mathematics Subject Classification*: Primary 11B39.
Keywords: Lucas sequences, indices.

(Concerned with sequence A006521, A014662, A016089, A023172, A057719, A091317, A129729, and A140409.)

Received August 21 2009; revised version received January 29 2010. Published in *Journal of Integer Sequences*, January 31 2010.

Return to Journal of Integer Sequences home page.