Publ. Math. Debrecen
58 / 1-2 (2001), 121–155

Multiply perfect numbers in Lucas sequences with odd parameters

By FLORIAN LUCA (Praha)

Abstract. Let $P > 0$ and Q be odd coprime integers such that $P^2 + 4Q > 0$. Let $(W_n)_{n \geq 0}$ be anyone of the two Lucas sequences with parameters P and Q. In this paper, we show that there are only finitely many n's such that W_n is multiply perfect; that is, $W_n \mid \sigma(W_n)$, where σ denotes the divisor sum function. Moreover, all such n's are, at least in theory, effectively computable.

1. Introduction

For any positive integer n let $\sigma(n)$ be the sum of the divisors of n. A positive integer n is called *multiply perfect* if $\sigma(n) = kn$ for some positive integer k. When $k = 2$, n is called *perfect*. Two positive integers m and n are called *amicable* if $\sigma(m) = \sigma(n) = m + n$. Notice that a positive integer n is self-amicable if and only if n is perfect.

In [13], we showed that there are no perfect Fibonacci and Lucas numbers and in [14], we showed that no two members of the Pell sequence are amicable. Various equations and inequalities involving the sum of divisors function σ and the Euler function ϕ of members of binary recurrence sequences were studied by us in [6–11] and [12].

In this paper, we study the problem of the occurence of multiply perfect numbers in Lucas sequences with odd parameters whose characteristic equation has real roots.

Mathematics Subject Classification: 11A25, 11B39, 11D61.
Key words and phrases: multiply perfect number, Lucas sequence, primitive divisor, square class.

Let $P > 0$ and Q be odd coprime integers such that $P^2 + 4Q > 0$. Let $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ be the Lucas sequences of the first and second kind respectively, given by $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$ and

$$\begin{aligned} U_{n+2} &= PU_{n+1} + QU_n, \\ V_{n+2} &= PV_{n+1} + QV_n \end{aligned} \qquad \text{for all } n \geq 0. \tag{1}$$

In what follows, we denote anyone of the two sequences $(U_n)_{n\geq 0}$ or $(V_n)_{n\geq 0}$ by $(W_n)_{n\geq 0}$. The above assumption $P > 0$ is only meant to insure that W_n is positive for all $n > 0$. However, the main result of this work applies when $P < 0$ as well if one replaces the sequence $(W_n)_{n\geq 0}$ by $(|W_n|)_{n\geq 0}$.

We have the following:

Theorem. *There exists an effectively computable constant C depending on P and Q, such that if W_n is multiply perfect, then $n < C$.*

Since the classical Fibonacci and Lucas sequences $(F_n)_{n\geq 0}$ and $(L_n)_{n\geq 0}$ are simply the two Lucas sequences corresponding to $P = Q = 1$, it follows that there are only finitely many effectively computable multiply perfect Fibonacci and Lucas numbers. Unfortunately, by using our method, the effectively computable constant C (should anyone dare to compute it) claimed by the Theorem is certainly too large to allow testing.

It is likely that our Theorem holds for Lucas sequences with even PQ as well. Unfortunately, for such sequences we could not deal with the case in which n is a power of 2, but we can show that there exist only finitely many n's, $n \neq 2^s$ for which W_n is multiply perfect.

Finally, notice that the Theorem may certainly fail if one removes the condition that P and Q are coprime. Indeed, the sequence

$$2^{n-1}(2^n - 1) = \frac{4^n - 2^n}{4 - 2}$$

is a Lucas look-alike sequence which, as far as we know, could contain infinitely many perfect numbers providing that there exist infinitely many Mersenne primes.

2. Notations and outline of the paper

Throughout this paper, when we refer at something being bounded in terms of something else, we mean bounded above.

For us, the number n will usually be written as $n = 2^s m$, where $s \geq 0$ and $m \geq 1$ is odd.

We use p, q and r to denote prime numbers. To avoid confusion, we always use p for a prime divisor of W_n, q for a prime divisor of n and r for a prime number which is, in general, unrelated to either n or W_n.

We use $\square$ to denote a perfect square. For two integers a and b such that $b \geq 1$ is odd, we use $\left(\frac{a}{b}\right)$ to denote the Jacobi symbol of a with respect to b.

For a positive integer n we denote by $\sigma(n)$, $\phi(n)$, $\Omega(n)$, $\omega(n)$ and $q(n)$ the sum of divisors function of n, the Euler ϕ function of n, the total number of prime divisors of n (counting multiplicities), the number of distinct prime divisors of n and the smallest prime dividing n, respectively. We also denote by $\Omega_o(n)$ and $\omega_o(n)$ the total number of odd prime divisors of n and the number of distinct odd prime divisors of n, respectively. So, in this paper, $\omega(n) - 1 \leq \omega_o(n) \leq \omega(n)$ and $\Omega_o(n) = \Omega(n) - s = \Omega(n) - \mathrm{ord}_2(n)$.

A few words about how this paper is organized.

In Section 3, we derive various upper bounds on $\sigma(W_n)/W_n$, first in terms of n, second in terms of the prime divisors of n and finally in terms of $\omega(n)$. In particular, we show that $\log\left(\frac{\sigma(W_n)}{W_n}\right)$ can be bounded quadratically in $\log(\omega(n))$. The arguments employed in this section use the theory of primitive divisors of $(W_n)_{n\geq 0}$ as developed by Carmichael in [2].

In Section 4, we investigate the equation

$$W_n = d\square, \tag{2}$$

where d is some positive integer. We may assume that d is square-free. By using the finite square-class theory for the sequence $(W_n)_{n\geq 0}$ as developed throughout [3], [4], [17]–[22] and [24]–[25], we show that if n and d satisfy equation (2), then $\Omega(n)$ can be bounded linearly in $\omega(d)$, at least when $W_n = U_n$. Our bound on $\Omega(n)$ in terms of $\omega(d)$ when $W_n = V_n$ is a bit worse involving also an extra term which may be exponential in s.

In Section 5, we give the proof of the Theorem. Assume that W_n is multiply perfect for some positive integer n. Let k be the ratio of $\sigma(W_n)$ to W_n. We begin by analyzing the order at which 2 can divide $\sigma(W_n)$. This is certainly bounded by $\log_2 k + \delta s + C$, where C is a constant and $\delta = 0$ or 1 according to whether $W_n = V_n$ or U_n. In particular, if one writes $W_n = d\,\square$, then $\omega(d)$ can be bounded linearly in $\log k$ and δs. From the results of Section 4, it follows that $\omega(n)$ can be bounded linearly in $\log_2 k + \delta s$. On the other hand, from the results of Section 3, we know that $\log k$ is bounded quadratically in $\log(\omega(n))$. Combining these two inequalities, we get that $\omega(n)$ is bounded. By combining various other technical inequalities scattered throughout Sections 3 and 4, we show that all three parameters k, $\Omega(n)$ and $q(n)$ are bounded by a computable constant, call it C. We conclude the proof by presenting an algorithm which determines, in C steps, a finite set of integers containing all the possible candidates n.

The constant C above is usually not that bad. Preliminary computations seem to indicate that $C < 200$, when $P = Q = 1$; that is, when one looks at the classical Fibonacci and Lucas sequences. However, from the way the final algorithm is designed, the size of the largest returned integer n is of the order of magnitude at least

$$\underbrace{\exp\exp\ldots\exp}_{C \text{ times}}(C).$$

Thus, if one really wants to compute all the multiply perfect Fibonacci or Lucas numbers, then one should probably come up with a better argument than the one presented in this paper.

Throughout the paper, we denote by C_1, C_2, ... effectively computable constants depending only on P and Q. Although Sections 3 and 4 are independent of each other and of Section 5, we keep labeling the constants in an increasing order throughout the whole paper.

The idea of this paper first came to us while listening to the talk *Perfect Number Pairs* presented by Professor H. HARBORTH at the Eigth International Conference on Fibonacci Numbers (see [5]). In that talk, the speaker presented some results concerning various arithmetic pairs, some of them involving terms from some binarry recurrence sequences. At that point, it occurred to us that maybe combining the primitive divisor theory with the square-class theory for the Fibonacci sequence, one could prove

our Theorem at least for the Fibonacci sequence. Thanks to the recent work [21], we could do this in a very general context.

We would like to thank several people whose input had, in some way or another, contributed to this work. I especially thank Professors J.H.E. Cohn, P. Corvaja, H. Harborth, P. Ribenboim, T.N. Shorey, L. Somer and U. Zannier for helpful correspondence. I also thank Dr. A. Flammenkamp for an interesting conversation concerning the behaviour of the sum (23) in terms of n and Professors Y. Bugeaud and A. Pethő for helpful advice concerning the proof of Proposition 2. Finally, I thank Professor A. Dress and the Mathematics Department in Bielefeld for their hospitality during the period when this paper was written and the Alexander von Humboldt Foundation for support.

3. Upper bounds for $\sigma(W_n)/W_n$

All the results of this section apply to all nondegenerate Lucas sequences regardless of the parities of P and Q or of the sign of the discriminant once one replaces W_n by $|W_n|$. We shall treat only the case of positive discriminant and we shall point out where the arguments can be adapted to treat the general case.

Let $n \geq 2$. We first treat the sequence $(W_n)_{n\geq 0} \equiv (U_n)_{n\geq 0}$ and we shall return to the sequence $(V_n)_{n\geq 0}$ later.

A *primitive divisor* p of U_n is a prime number p such that $p \mid U_n$ but $p \nmid U_m$ for any $m < n$. By results of Carmichael (see [2]), we know that U_n has a primitive divisor for all $n \geq 2$, except maybe for $n = 2, 3, 6, 12$. We note that Carmichael's result was recently extended to arbitrary Lucas sequences in [1].

For any positive integer n let $\mathcal{P}_n$ be the set of primitive divisors of U_n. It is well-known that if $p \in \mathcal{P}_n$, then $p \equiv e_p \pmod{n}$, where $e_p = \left(\frac{p}{P^2+4Q}\right)$.

Let

$$\alpha = \frac{P + \sqrt{P^2+4Q}}{2} \quad \text{and} \quad \beta = \frac{P - \sqrt{P^2+4Q}}{2} \tag{3}$$

be the two roots of the characteristic equation

$$x^2 - Px - Q = 0. \tag{4}$$

Notice that $\alpha > |\beta| > 0$. Since

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for all } n \geq 0, \tag{5}$$

it follows, in particular, that

$$U_n < 2\alpha^n \quad \text{for all } n \geq 0. \tag{6}$$

Notice that if $(U_n)_{n\geq 0}$ is an arbitrary Lucas sequence, then by making the convention that $|\alpha| \geq |\beta|$, one still has that the inequality $|U_n| \leq 2|\alpha|^n$ holds for all $n \geq 0$.

Let $d \mid n$ be a divisor of n. Assume $d > 2$. Let $l(d)$ be the cardinality of $\mathcal{P}_d$ and let $p_1(d) < \cdots < p_{l(d)}(d)$ be all the primes in $\mathcal{P}_d$. Since

$$\prod_{i=1}^{l(d)} p_i(d) \mid U_d,$$

it follows that

$$\sum_{i=1}^{l(d)} \log(p_i(d)) \leq \log(U_d) < \log(2\alpha^d) = \log 2 + d\log\alpha. \tag{7}$$

Since $p_1(d) \geq d - 1$, it follows that

$$l(d)\log(d-1) < \log 2 + d\log\alpha$$

or

$$l(d) < \frac{1}{\log(d-1)}(\log 2 + d\log\alpha). \tag{8}$$

Now write

$$U_n = \prod_{\substack{d\mid n\\ d>1}} \prod_{p\in\mathcal{P}_d} p^{\alpha_p} \tag{9}$$

where α_p is the exponent at which p appears in U_n. Since

$$\frac{\sigma(k)}{k} \leq \frac{k}{\phi(k)} \quad \text{for all } k \geq 1,$$

it follows that

$$\frac{\sigma(U_n)}{U_n} \leq \frac{U_n}{\phi(U_n)} = \prod_{\substack{d|n \\ d>1}} \prod_{i=1}^{l(d)} \left(1 + \frac{1}{p_i(d)-1}\right).$$

Hence,

$$\frac{\sigma(U_n)}{U_n} \leq x_n \prod_{\substack{d|n \\ d>2}} \prod_{i=1}^{l(d)} \left(1 + \frac{1}{p_i(d)-1}\right), \tag{10}$$

where

$$x_n = \begin{cases} 1 & \text{if } 2 \nmid n \text{ and} \\ \dfrac{U_2}{\phi(U_2)} & \text{if } 2 \mid n. \end{cases} \tag{11}$$

By taking logarithms in (10), we get

$$\begin{aligned} \log\left(\frac{\sigma(U_n)}{U_n}\right) &\leq \log x_n + \sum_{\substack{d|n \\ d\geq 3}} \sum_{i=1}^{l(d)} \log\left(1 + \frac{1}{p_i(d)-1}\right) \\ &< \log x_n + \sum_{\substack{d|n \\ d\geq 3}} \sum_{i=1}^{l(d)} \frac{1}{p_i(d)-1}. \end{aligned} \tag{12}$$

Fix $d \geq 3$. We find an upper bound for the sum

$$\sum_{i=1}^{l(d)} \frac{1}{p_i(d)-1}. \tag{13}$$

Notice first that since $p_i(d) \equiv 0, \pm 1 \pmod{d}$, it follows that $p_1(d) \geq d-1$, $p_2(d) \geq d$, $p_3(d) \geq 2d-1$, $p_4(d) \geq 2d+1$ and so on. In particular,

$$p_i(d) - 1 > \frac{id-2}{2} \quad \text{for all } i = 1, \ldots, l(d). \tag{14}$$

Hence,

$$\sum_{i=1}^{l(d)} \frac{1}{p_i(d)-1} < 2\sum_{i=1}^{l(d)} \frac{1}{id-2} \le 2\left(\frac{1}{d-2} + \int_1^{l(d)} \frac{dy}{yd-2}\right) \tag{15}$$
$$= 2\left(\frac{1}{d-2} + \frac{1}{d}\log\left(\frac{l(d)d-2}{d-2}\right)\right).$$

Hence,

$$\sum_{i=1}^{l(d)} \frac{1}{p_i(d)-1} < 2\left(\frac{1}{d-2} + \frac{1}{d}\log\left(\frac{l(d)d}{d-2}\right)\right). \tag{16}$$

Combining inequalities (8) and (16), we get

$$\sum_{i=1}^{l(d)} \frac{1}{p_i(d)-1} < 2\left(\frac{1}{d-2} + \frac{1}{d}\log\left(\frac{d(\log 2 + d\log\alpha)}{(d-2)\log(d-1)}\right)\right). \tag{17}$$

Let $C_1 > 2$ be such that

$$\frac{1}{x-2} + \frac{1}{x}\log\left(\frac{x(\log 2 + x\log\alpha)}{(x-2)\log(x-1)}\right) < \frac{\log x}{x} \quad \text{for } x > C_1. \tag{18}$$

It is clear that such a constant exists since the function appearing on the left side of inequality (18) decreases faster than the one appearing on the right side of inequality (18).

Let

$$C_2 = \sum_{3\le k\le C_1} 2\left(\frac{1}{k-2} + \frac{1}{k}\log\left(\frac{k(\log 2 + k\log\alpha)}{(k-2)\log(k-1)}\right)\right). \tag{19}$$

Set

$$C_3 = C_2 + \log\left(\frac{U_2}{\phi(U_2)}\right) \tag{20}$$

and

$$u_n = \begin{cases} 0 & \text{if } q(n) > C_1, \\ C_3 & \text{otherwise.} \end{cases} \tag{21}$$

From inequality (12) and formulae (16)–(21), it follows that

$$\log\left(\frac{\sigma(U_n)}{U_n}\right) < u_n + 2\sum_{\substack{d|n\\ d>C_1}} \frac{\log d}{d} < u_n + 2\sum_{d|n} \frac{\log d}{d}. \tag{22}$$

Notice that bound (22) depends on n alone.

We now use inequality (22) to find an upper bound for $\log(\sigma(U_n)/U_n)$ in terms of the prime divisors of n only. In order to do this, we investigate the sum

$$\sum_{d|n} \frac{\log d}{d}. \tag{23}$$

Unfortunately, the function $\log n/n$ is not multiplicative, so one should not expect a nice formula for the sum (23) in terms of n.

For any positive integer m let $f(m) = \sigma(m)/m$. For every prime power q^β let

$$S(q^\beta) = \frac{1}{q} + \frac{2}{q^2} + \cdots + \frac{\beta}{q^\beta}. \tag{24}$$

We have the following result:

Lemma 1. *Assume that $n = q_1^{\beta_1} \cdot \ldots \cdot q_t^{\beta_t}$ is the decomposition of n in distinct prime powers. Then,*

$$\sum_{d|n} \frac{\log d}{d} = \sum_{j=1}^{t} \log(q_j) S\left(q_j^{\beta_j}\right) f\left(\frac{n}{q_j^{\beta_j}}\right). \tag{25}$$

Proof of Lemma 1. When $t = 1$, one gets

$$\sum_{d|n} \frac{\log d}{d} = \sum_{l=1}^{\beta_1} \frac{\log q_1^l}{q_1^l} = \log q_1 \sum_{l=1}^{\beta_1} \frac{l}{q_1^l} = \log q_1 S\left(q_1^{\beta_1}\right) f(1). \tag{26}$$

Hence, formula (25) holds for $t = 1$. One can now easily use induction to prove that (25) holds for all $t \geq 2$. We do not give further details. □

By noticing that

$$S(q^\beta) = \frac{1}{q} + \frac{2}{q^2} + \cdots + \frac{\beta}{q^\beta} < \left(1 + \frac{1}{q} + \cdots + \frac{1}{q^\beta}\right) \cdot \left(\frac{1}{q} + \frac{1}{q^2} + \cdots + \frac{1}{q^\beta}\right) < \frac{2}{q-1}$$

holds for all $\beta \geq 1$ and $q \geq 2$, it follows, by Lemma 1, that

$$\sum_{d|n} \frac{\log d}{d} < 2f(n)\left(\sum_{q|n} \frac{\log q}{(q-1)}\right). \tag{27}$$

In particular, inequality (27) implies

$$\sum_{d|n} \frac{\log d}{d} < 2\left(\sum_{q|n} \frac{\log q}{q-1}\right) \prod_{q|n} \left(1 + \frac{1}{q-1}\right). \tag{28}$$

Combining (28) with (22), we get

$$\log\left(\frac{\sigma(U_n)}{U_n}\right) < u_n + 4\left(\sum_{q|n} \frac{\log q}{q-1}\right) \prod_{q|n} \left(1 + \frac{1}{q-1}\right). \tag{29}$$

This gives an upper bound for $\log(\sigma(U_n)/U_n)$ in terms of the prime factors of n.

Finally, we use (29) to derive an upper bound for $\log(\sigma(U_n)/U_n)$ in terms of the number $\omega(n)$ of prime factors of n.

Suppose that $t = \omega(n)$ and that $q_1 < q_2 < \cdots < q_t$ are all the distinct primes dividing n. Then, certainly $q_i \geq r_i$, where r_i is the i'th prime. From Theorems 3, 6 and 8 in [23], we know that there exist two constants C_4 and C_5 such that

$$\prod_{i=1}^{t} \left(1 + \frac{1}{r_i - 1}\right) < C_4 \log(t+1) \tag{30}$$

and

$$\sum_{i=1}^{t} \frac{\log r_i}{r_i - 1} < C_5 \log(t+1). \tag{31}$$

Combining inequalities (29)–(31) with the fact that the function $x \to \log x/(x-1)$ is decreasing for $x \geq 2$, we get

$$\sum_{d|n} \frac{\log d}{d} < C_6 \log^2(\omega(n)+1) \tag{32}$$

and

$$\log\left(\frac{\sigma(U_n)}{U_n}\right) < u_n + C_7 \log^2(\omega(n)+1), \tag{33}$$

where $C_6 = C_4 \cdot C_5$ and $C_7 = 4C_6$.

This concludes our discussion concerning upper bounds for $\sigma(U_n)/U_n$ in terms of n.

We now treat the sequence $(V_n)_{n\geq 0}$. First of all, by the same work of Carmichael [2], we know that V_n has a primitive divisor for all $n \geq 2$, except maybe for $n = 2, 3, 6$. Moreover, if p is a primitive divisor of V_n, then $p \equiv 0, \pm 1 \pmod{n}$. Since inequality (6) holds for U_n replaced by V_n as well, it follows that the arguments employed for the sequence $(U_n)_{n\geq 0}$ extend to the sequence $(V_n)_{n\geq 0}$. In particular, inequalities (29) and (33) translate in

$$\log\left(\frac{\sigma(V_n)}{V_n}\right) < v_n + 4\left(\sum_{q|n} \frac{\log q}{q-1}\right) \prod_{q|n} \left(1 + \frac{1}{q-1}\right) \tag{34}$$

and

$$\log\left(\frac{\sigma(V_n)}{V_n}\right) < v_n + C_7 \log^2(\omega(n)+1), \tag{35}$$

where v_n has the same formula as u_n (see formulae (20)–(21)) with U_2 replaced by V_2. Bounds (34) and (35) cannot be much improved (at least not by using the present method) when n is odd. When $2 \parallel n$, then inequality (34) holds with the factor 4 replaced by the factor 2 in front of the product appearing at the right side and inequality (35) holds with C_7 reduced by a factor of 2. However, the bounds (34) and (35) can be a lot strengthened when n happens to be divisible with a large power of 2. Indeed, the arguments employed for dealing with the sequence $(U_n)_{n\geq 0}$, were based on the fact that $U_d \mid U_n$ whenever $d \mid n$, whereas $V_d \mid V_n$ if and only if $d \mid n$ and n/d is odd.

Let us assume that $n = 2^s m$ where s is large (in a sense that will be made more precise later) and m is odd. Write

$$V_m = V_{2^s m} = V_{2^s} \cdot \frac{V_n}{V_{2^s}}. \tag{36}$$

For simplicity, denote

$$V'_m = \frac{V_n}{V_{2^s}} = \frac{(\alpha^{2^s})^m + (\beta^{2^s})^m}{(\alpha^{2^s}) + (\beta^{2^s})}. \tag{37}$$

Using the fact that

$$f(k_1k_2) = \frac{\sigma(k_1k_2)}{k_1k_2} \le \frac{\sigma(k_1)\sigma(k_2)}{k_1k_2} = f(k_1)f(k_2) \quad \text{for all } k_1,\ k_2 \ge 1, \tag{38}$$

we get

$$\log\left(\frac{\sigma(V_n)}{V_n}\right) \le \log\left(\frac{\sigma(V_{2^s})}{V_{2^s}}\right) + \log\left(\frac{\sigma(V'_m)}{V'_m}\right). \tag{39}$$

We first analyze the term in V'_m. Notice that for fixed s and variable m, the part of the sequence $(V'_m)_{m\ge 0}$ for m odd is a part of a Lucas sequence of the first kind whose characteristic equation has the roots α^{2^s} and β^{2^s}. Fix m odd. Let $d \mid m$ and denote by $\mathcal{P}'_d$ to be the set of primitive divisors of V'_d. Assume that $\mathcal{P}'_d$ consists of $l'(d)$ elements namely $p'_1(d) < \cdots < p'_{l'(d)}(d)$. In this case, each one of the primes p'_i is congruent to 0 or ± 1 modulo $2^{s+1}d$. The arguments employed at formulae (13)–(17), show that

$$\sum_{i=1}^{l'(d)} \frac{1}{p'_i(d)-1} < 2\left(\frac{1}{2^{s+1}d-2} + \frac{1}{2^{s+1}d}\log\left(\frac{2^{s+1}d(\log 2 + 2^{s+1}d\cdot 2^s\log\alpha)}{(2^{s+1}d-2)\log(2^{s+1}d-1)}\right)\right). \tag{40}$$

Let C_8 and C_9 be two constants such that

$$2\left(\frac{1}{2^{s+1}d-2} + \frac{1}{2^{s+1}d}\log\left(\frac{2^{s+1}d(\log 2 + 2^{s+1}d\cdot 2^s\log\alpha)}{(2^{s+1}d-2)\log(2^{s+1}d-1)}\right)\right) < \frac{C_8}{1.5^s}\cdot\frac{\log d}{d}, \tag{41}$$

for all $s \ge C_9$ and $d \ge 3$. The arguments employed for the sequence $(U_n)_{n\ge 0}$ show that

$$\log\left(\frac{\sigma(V'_m)}{V'_m}\right) < \frac{C_8}{1.5^s}\left(v'_m + 4\left(\sum_{q\mid m}\frac{\log q}{q-1}\right)\prod_{q\mid m}\left(1+\frac{1}{q-1}\right)\right) \tag{42}$$

and

$$\log\left(\frac{\sigma(V'_m)}{V_m}\right) < \frac{C_8}{1.5^s}\left(v'_m + C_7\log^2(\omega(m)+1)\right), \tag{43}$$

whenever $s > C_9$, where $v'_m = C_3$ if $q(m) \le C_1$ and $v'_m = 0$ otherwise.

By employing the previous arguments, one can also check easily that

$$\log\left(\frac{\sigma(V_{2^s})}{V_{2^s}}\right) < \frac{C_8}{1.5^s} \quad \text{for } s > C_{10}. \tag{44}$$

Assuming $C_9 > C_{10}$ (if not, simply replace C_9 by C_{10}), we get, by inequalities (39), (42) and (43), that

$$\log\left(\frac{\sigma(V_n)}{V_n}\right) < \frac{1}{1.5^s}\left(C_8 v'_m + C_{11}\left(\sum_{q|m}\frac{\log q}{q-1}\right)\prod_{q|m}\left(1+\frac{1}{q-1}\right)\right) \tag{45}$$

and

$$\log\left(\frac{\sigma(V_n)}{V_n}\right) < \frac{1}{1.5^s}\left(C_8 v'_m + C_{12}\log^2(\omega(m)+1)\right), \tag{46}$$

for some constants C_{11} and C_{12}, whenever $s > C_9$.

This ends our discussion about upper bounds for $\sigma(V_n)/V_n$. In the proof of the Theorem, we shall use formulae (34)–(35) to deal with the case in which s is small ($s \le C_9$) and formulae (45)–(46) to deal with the case in which s is large ($s > C_9$).

We conclude this section by noticing that, in fact, we proved the following:

Proposition 1. *Let $(W_n)_{n\ge 0}$ be an arbitrary Lucas sequence. Then, there exists a constant C such that*

$$\sum_{p|W_n}\frac{1}{p} < C\log^2(\omega(n)+1) \quad \textit{for all } n \ge 1. \tag{47}$$

4. The equation $W_n = d\square$

In this section, we analyze the equation

$$W_n = d\square, \tag{48}$$

when d is a square-free positive integer. More precisely, we are interested in obtaining upper bounds for $\Omega(n)$ in terms of $\omega(d)$.

We begin by recalling the theory of square-classes of Lucas sequences as developed throughout [3], [4], [17]–[22] and [24]–[25]. For a fixed positive integer k, the square class of k with respect to the sequence $(W_n)_{n\geq 0}$ is defined as being the set of all positive integers m such that $W_k \cdot W_m = \square$. In the above definition, we do not allow the value of m or k to be zero when working with the sequence $(W_n)_{n\geq 0} \equiv (U_n)_{n\geq 0}$, mainly because otherwise $W_0 = U_0 = 0$ would be in every square-class. A square-class is called *trivial* if it consists of only one element. We warn the reader that most authors consider the square class of k with respect to $(W_n)_{n\geq 0}$ as being the set of all W_m's such that $W_k \cdot W_m = \square$; that is, they consider the square-class as consisting of the members of $(W_n)_{n\geq 0}$ rather than of the indices of those members. Since we are interested in arithmetical propertices of the indices, we adopt the convention that a square-class is a set of indices.

We need several lemmas and propositions.

Lemma 2. 1. *There are only finitely many non-trivial square-classes with respect to the sequence* $(W_n)_{n\geq 0}$.

2. *Each square-class consists of at most three terms.*

Proof of Lemma 2. See, for example, [17], [22] or [25].

In fact, in [22], McDaniel and Ribenboim have given a very precise description of most non-trivial square-classes that $(W_n)_{n\geq 0}$ might have. □

Proposition 2. *Let D and s be any two fixed positive integers such that $s > 1$. Then, the equation*

$$\frac{U_{sm}}{U_m} = D\square \tag{49}$$

has only finitely many solutions m and all of them are effectively computable in terms of s, D, P and Q. If s is odd, then the above statement remains true if in equation (49) *one replaces the terms of the sequence $(U_n)_{n\geq 0}$ by the corresponding terms of the sequence $(V_n)_{n\geq 0}$.*

Proof Proposition 2 (based on an idea of Y. Bugeaud). If $s = 2$, then one simply obtains the equation $V_m = D\square$. The fact that this equation has only finitely many effectively computable solutions m follows,

for example, from a result obtained independently by PETHŐ (see [17]) and SHOREY and STEWART (see [25]).

Assume now that $s \geq 4$. Rewrite equation

$$\frac{U_{ms}}{U_m} = \frac{\alpha^{ms} - \beta^{ms}}{\alpha^m - \beta^m} = Dx^2 \tag{50}$$

as

$$\frac{X^s - 1}{X - 1} = DY^2, \tag{51}$$

where

$$X = \left(\frac{\alpha}{\beta}\right)^m \quad \text{and} \quad Y = \frac{x}{\beta^{(m(s-1)/2)}}. \tag{52}$$

Let $\mathbb{K} = \mathbb{Q}[\alpha^{1/2}, \beta^{1/2}]$ and let S be the set of all prime ideals in $\mathbb{K}$ dividing β. Since $s \geq 4$, it follows that the polynomial

$$\frac{X^s - 1}{X - 1} \tag{53}$$

has at least three simple roots. In fact, notice that all the roots of the polynomial given by formula (53) are precisely $e^{2i\pi k/s}$ for $k = 1, 2, \ldots, s-1$. Hence, they are all distinct. Now the fact that equation (51) has only finitely many effectively computable solutions of the form (52) follows from the general theory of S-integer points on hyperelliptic curves (see, for example, [26]).

Assume now that $s = 3$. In this case, equation (49) is

$$\alpha^{2m} + (\alpha\beta)^m + \beta^{2m} = Dx^2,$$

or

$$3V_m^2 + \Delta U_m^2 = D(2x)^2, \tag{54}$$

where $\Delta = P^2 + 4Q = (\alpha - \beta)^2$.

We first analyze the equation

$$3X^2 + \Delta Y^2 = DZ^2. \tag{55}$$

From a result of D.W. Masser (see the Proposition on page 26 in [15]), we know that if equation (55) has a solution in integers X, Y, Z with $XYZ \neq 0$, then it has one satisfying

$$\max(|X|, |Y|, |Z|) < (9 + 3\Delta + 3D)^{1.5}. \tag{56}$$

Let $K = (9 + 3\Delta + 3d)^{1.5}$. If equation (55) does not have any solutions with

$$\max(|X|, |Y|, |Z|) < K,$$

then equation (54) does not have any solutions either and the problem is solved.

Assume now that equation (55) has a solution with $XYZ \neq 0$. Let $X = X_0$, $Y = Y_0$, $Z = Z_0$ be a positive solution of (55) with $\gcd(X_0, Y_0, Z_0) = 1$ and

$$\max(X_0, Y_0, Z_0) < K.$$

We begin by finding all the rational points on the curve

$$Dz^2 - \Delta y^2 = 3. \tag{57}$$

Since $z_0 = Z_0/X_0$ and $y_0 = Y_0/X_0$ is a rational point on the curve (57), it follows that one can parametrize all rational solutions of equation (57) simply by letting

$$t = \frac{z - z_0}{y - y_0}$$

and computing z and y versus z_0, y_0 and t from equation (57). The resulting formulae are:

$$\begin{cases} y = \dfrac{y_0 Dt^2 - 2z_0 Dt + y_0\Delta}{Dt^2 - \Delta}, \\ z = \dfrac{-z_0 Dt^2 + 2y_0\Delta t - z_0\Delta}{Dt^2 - \Delta}. \end{cases} \tag{58}$$

Clearly, t is a rational number. Notice moreover that the above formulae are correctly defined in the sense that the denominator $Dt^2 - \Delta$ can never vanish. Indeed, a straightforward computation shows that the conditions

$$\begin{cases} Dt^2 - \Delta = 0 \\ y_0 Dt^2 - 2z_0 Dt + y_0\Delta = 0 \end{cases}$$

force $Dz_0^2 - \Delta y_0^2 = 0$, which is impossible because the point (z_0, y_0) is on the curve given by formula (57).

Assume now that X, Y, Z are nonzero integers satisfying equation (55). Since the point of coordinates $z = Z/X$ and $y = Y/X$ is a rational point on the curve (57), it follows that there exists some rational number $t = u/v$ with u and v coprime such that formulae (58) are satisfied. Hence,

$$\begin{cases} \dfrac{Y}{X} = \dfrac{u^2DY_0 - 2uvDZ_0 + v^2\Delta Y_0}{(u^2D - v^2\Delta)X_0}, \\ \dfrac{Z}{X} = \dfrac{-u^2DZ_0 + 2uv\Delta Y_0 - v^2\Delta Z_0}{(u^2D - v^2\Delta)X_0}. \end{cases} \tag{59}$$

Let $d = \gcd(X, Y, Z)$. From equations (59), it follows that

$$\begin{cases} X = \dfrac{d}{d_1}(u^2D - v^2\Delta)X_0, \\ Y = \dfrac{d}{d_1}(u^2DY_0 - 2uvDZ_0 + v^2\Delta Y_0), \\ Z = \dfrac{d}{d_1}(-u^2DZ_0 + 2uv\Delta Y_0 - v^2\Delta Z_0). \end{cases} \tag{60}$$

In formula (60), we used d_1 for the greatest common divisor of all three numbers

$$(u^2D - v^2\Delta)X_0, \;\; u^2DY_0 - 2uvDZ_0 + v^2\Delta Y_0, \;\; -u^2DZ_0 + 2uv\Delta Y_0 - v^2\Delta Z_0.$$

Notice first of all that all prime divisors of d_1 divide $6D\Delta X_0$.

Indeed, to see why this is so, assume that p does not divide $6D\Delta X_0$ but

$$u^2D \equiv v^2\Delta \pmod{p} \tag{61}$$

and

$$u^2DY_0 - 2uvDZ_0 + v^2\Delta Y_0 \equiv 0 \pmod{p}. \tag{62}$$

If we substitute (61) in (62), we get

$$v^2\Delta Y_0 - 2uvDZ_0 + v^2\Delta Y_0 \equiv 0 \pmod{p}$$

or

$$2v^2\Delta Y_0 \equiv 2uvDZ_0 \pmod{p}. \tag{63}$$

Notice that p does not divide uv. Indeed, if for example $p \mid u$, then since $(u, v) = 1$ formula (61) would imply that $p \mid \Delta$, which contradicts the fact that p does not divide $6D\Delta X_0$. Now from formula (63) we get that

$$v\Delta Y_0 \equiv uDZ_0 \pmod{p}$$

or, after squaring both sides of the above congruence,

$$(v^2\Delta)(\Delta Y_0^2) \equiv (u^2D)(DZ_0^2) \pmod{p}. \tag{64}$$

From formulae (61) and (64) we get that

$$\Delta Y_0^2 \equiv DZ_0^2 \pmod{p}$$

or

$$3X_0^2 = DZ_0^2 - \Delta Y_0^2 \equiv 0 \pmod{p},$$

which is the desired contradiction.

Let us now return to equation (54). From the above considerations we get that

$$\begin{cases} U_m = \dfrac{d}{d_1}(u^2DY_0 - 2uvDZ_0 + v^2\Delta Y_0), \\ V_m = \dfrac{d}{d_1}(u^2D - v^2\Delta)X_0. \end{cases} \tag{65}$$

Notice first of all that $d \mid (U_m, V_m)$; hence $d \mid 4Q^m$ (for a proof of this well-known fact see, for example, [16]). Formula (65) can be rewritten as

$$\begin{cases} \alpha^m - \beta^m = \dfrac{d\sqrt{\Delta}}{d_1}(u^2DY_0 - 2uvDZ_0 + v^2\Delta Y_0), \\ \alpha^m + \beta^m = \dfrac{d}{d_1}(u^2D - v^2\Delta)X_0. \end{cases} \tag{66}$$

Hence,

$$\begin{cases} 2\alpha^m = \dfrac{d}{d_1}\big(u^2D(X_0 + \sqrt{\Delta}Y_0) - 2uvD\sqrt{\Delta}Z_0 - v^2\Delta(X_0 - \sqrt{\Delta}Y_0)\big), \\ 2\beta^m = \dfrac{d}{d_1}\big(u^2D(X_0 - \sqrt{\Delta}Y_0) + 2uvD\sqrt{\Delta}Z_0 - v^2\Delta(X_0 + \sqrt{\Delta}Y_0)\big). \end{cases} \tag{67}$$

Denote

$$\begin{cases} f_1(u,v)=u^2D(X_0+\sqrt{\Delta}Y_0)-2uvD\sqrt{\Delta}Z_0-v^2\Delta(X_0-\sqrt{\Delta}Y_0), \\ f_2(u,v)=u^2D(X_0-\sqrt{\Delta}Y_0)+2uvD\sqrt{\Delta}Z_0-v^2\Delta(X_0+\sqrt{\Delta}Y_0). \end{cases} \tag{68}$$

Notice that by multiplying equations (67) we get that

$$4\frac{d_1^2}{d^2}(\alpha\beta)^m = f_1(u,v)f_2(u,v). \tag{69}$$

In equation (69), notice that the largest prime factor of the left side is bounded (this is because if p is a prime factor of the left side then either $p \mid 2d_1$, hence $p \mid 6D\Delta X_0$, or $p \mid (\alpha\beta) = -Q$). Thus, if we succeed in showing that the homogeneous form of degree four $f_1(u,v)f_2(u,v)$ has only simple factors, then the fact that equation (68) has only finitely many solutions will follow from the general theory of Thue equations (see, for example, [26]).

We first show that none of the quadratic forms $f_1(u,v)$ or $f_2(u,v)$ is a constant multiple of a perfect square. Notice that they both have the same discriminant namely

$$4(D^2\Delta Z_0^2 + D\Delta(X_0^2 - \Delta Y_0^2)). \tag{70}$$

If the expression given by formula (70) is zero, then

$$D\Delta(DZ_0^2 + X_0^2 - \Delta Y_0^2) = 0,$$

or

$$0 = (DZ_0^2 - \Delta Y_0^2) + X_0^2 = 3X_0^2 + X_0^2 = 4X_0^2,$$

which is impossible.

We now show that the two quadratic forms $f_1(u,v)$ and $f_2(u,v)$ are coprime. Assume that this is not the case. Then a common linear factor of them will divide both

$$u^2DY_0 - 2uvDZ_0 + v^2\Delta Y_0 \tag{71}$$

and

$$u^2D - v^2\Delta. \tag{72}$$

It now follows that for $v = 1$, the equation

$$u^2 DY_0 - 2uDZ_0 + \Delta Y_0 = 0 \tag{73}$$

will have as one of its solutions either $u = (\Delta/D)^{1/2}$ or $u = -(\Delta/D)^{1/2}$. We will treat only the case in which $u = (\Delta/D)^{1/2}$ is a solution of equation (72) as the remaining case is similar. We get

$$\frac{\Delta}{D} \cdot DY_0 - 2\left(\frac{\Delta}{D}\right)^{1/2} \cdot DZ_0 + \Delta Y_0 = 0,$$

or

$$\sqrt{\Delta} Y_0 = \sqrt{D} Z_0,$$

or

$$DZ_0^2 - \Delta Y_0^2 = 0,$$

which is impossible because $DZ_0^2 - \Delta Y_0^2 = 3X_0^2$.

Proposition 2 is therefore proved. □

Particular instances of Proposition 2 have been treated in various papers throughout the literature. For example in [17], [20] and [25], it is shown that the equation

$$W_m = D\,\square \tag{74}$$

has only finitely many solutions m and that all of them are effectively computable in terms of D, P and Q. In [21], McDaniel and Ribenboim have determined, in an elementary fashion, all solutions of equation (74) when $D = 1$ or 2. We also mention that Rotkiewicz (see [24]) showed that in some instances equation (49) has no solution when $s = D$ is prime. However, his results apply only for Lucas or Lehmer sequences for which one of the parameters P or Q is even.

We are now ready to prove some more lemmas and propositions that we need.

Lemma 3. *There are only finitely many pairs (q, m), where q is a prime for which*

$$\frac{U_{mq}}{U_m} = D\,\square \quad \text{or} \quad 2D\,\square \tag{75}$$

for some D which is divisible only with primes dividing P^2+4Q. Moreover, all such pairs are effectively computable in terms of P and Q.

The above statement remains true for pairs (q,m) such that $q \geq 3$ if in equation (75) *one replaces the terms of the sequence $(U_n)_{n\geq 0}$ by the corresponding terms of the sequence $(V_n)_{n\geq 0}$.*

Proof of Lemma 3. We treat only the sequence $(U_n)_{n\geq 0}$ since the corresponding statement for the sequence $(V_n)_{n\geq 0}$ can be dealt with similarly. We may also assume that D is square-free.

Assume first that $D = 1$. By either Lemma 2 or Proposition 2, it follows that there are only finitely many pairs (q,m), such that

$$\frac{U_{mq}}{U_m} = \square. \tag{76}$$

In fact, from the results from [22], we know that there is no such pair with $q > 3$, that there are at most two such pairs with $q = 2$ and only finitely many with $q = 3$.

Assume now that

$$\frac{U_{mq}}{U_m} = 2\square \tag{77}$$

for some prime number q. It follows easily that either $q = 2$ or $q = 3$. Hence, equation (77) can be written either as

$$V_m = \square \quad \text{or as} \quad \frac{U_{3m}}{U_m} = 2\square.$$

By either Lemma 2 or Proposition 2, it follows that there are only finitely many such m's. In fact, from either [21] or [22], it follows that there are at most three m's for which $V_m = \square$, namely $m = 1, 3$ or 5.

Assume now that

$$\frac{U_{mq}}{U_m} = D\square \quad \text{or} \quad 2D\square \tag{78}$$

for some $D \neq 1$, where $D \mid P^2 + 4Q = (\alpha - \beta)^2$. Let p be a prime number such that $p \mid D$. Notice that

$$\frac{U_{mq}}{U_m} = (\alpha^m)^{q-1} + (\alpha^m)^{q-2}(\beta^m) + \cdots + (\beta^m)^{q-1} \equiv \pm q \pmod{p}, \tag{79}$$

where the sign in (79) depends on whether or not q is a quadratic residue modulo p. Equations (78) and (79) imply that $q \equiv 0 \pmod{p}$. Hence, $q = p$ and equation (78) is

$$\frac{U_{mp}}{U_m} = p\square \quad \text{or} \quad 2p\square. \tag{80}$$

For each p fixed, it follows, by Proposition 2, that there are only finitely many m's for which either one of the equations (80) is satisfied. The claim of the Lemma follows now by noticing that there are only finitely many such p's (namely, the prime divisors of $P^2 + 4Q$).

Lemma 3 is therefore proved. □

We are now ready to treat equation (48) at least when $(W_n)_{n\geq 0} \equiv (U_n)_{n\geq 0}$.

Proposition 3. *There exists a computable constant C, such that if*

$$U_n = d\square, \tag{81}$$

then

$$\Omega(n) \leq \omega(d) + C. \tag{82}$$

Proof of Proposition 3. We may assume that d is square-free and that $\Omega(n)$ is large. Let C_{13} be an upper bound for the number of all pairs of the form (q, m) satisfying equation (75) for some square-free $D \mid P^2 + 4Q$. The existence of C_{13} is guaranteed by Lemma 3. The claim is that inequality (82) holds for $C = C_{13}$. Indeed, here is the argument.

Assume $\Omega(n) = t$ and let $q_1 \leq q_2 \leq \cdots \leq q_t$ be all the primes (counted with multiplicities) dividing n. Denote $m_0 = n$ and

$$m_i = \frac{n}{q_1 \dots q_i} = q_{i+1} \dots q_t \quad \text{for } i = 1, \dots, t-1. \tag{83}$$

Write equation (81) as

$$d\square = U_n = U_{m_0} = \frac{U_{m_0}}{U_{m_1}} \cdot \frac{U_{m_1}}{U_{m_2}} \cdot \ldots \cdot \frac{U_{m_{t-1}}}{U_{m_t}}. \tag{84}$$

From the way we have arranged the primes q_j, it can be easily seen that the greatest common divisor of any two of the factors appearing in the

product from the right hand side of formula (84) is divisible only with primes dividing $2(P^2+4Q)$. Indeed, assume that

$$p \mid \gcd\left(\frac{U_{m_i}}{U_{m_{i+1}}}, \frac{U_{m_j}}{U_{m_{j+1}}}\right) \tag{85}$$

for some $j > i$. In particular, $p \mid U_{m_j}$. Since $j \geq i+1$, it follows that $m_j \mid m_{i+1}$. Hence, $p \mid U_{m_{i+1}}$. In particular,

$$p \mid \gcd\left(\frac{U_{m_i}}{U_{m_{i+1}}}, U_{m_{i+1}}\right). \tag{86}$$

But it is well-known that the greatest common divisor appearing in formula (86) is a divisor of $m_i/m_{i+1} = q_{i+1}$. Hence, $p = q_{i+1}$. In particular, $p = q_{i+1} \mid U_{q_{i+1}(q_{i+1}^2-1)}$. Since $p \mid U_{m_j}$, it follows that

$$p = q_{i+1} \mid \gcd(U_{q_{i+1}(q_{i+1}^2-1)}, U_{m_j}) = U_{(q_{i+1}(q_{i+1}^2-1),\, m_j)}. \tag{87}$$

From formula (87), it follows that

$$\gcd(q_{i+1}(q_{i+1}^2-1), m_j) \neq 1. \tag{88}$$

However, from the fact that $m_j = q_{j+1}q_{j+2}\dots q_t$ and $q_{j+1} \geq q_{i+1}$, it follows, by formula (88), that either $q_{i+1} = q_{j+1}$, or $q_{i+1} = 2$ and $q_{j+1} = 3$. When $q_{i+1} = q_{j+1}$, formula (87) implies that $p = q_{i+1} \mid U_{q_{i+1}}$, which shows that p is a divisor of P^2+4Q. Finally, when $q_{i+1} = 2$ and $q_{j+1} = 3$, we simply get $2 = q_{i+1} = p$. This shows that indeed the greatest common divisor given by formula (85) is divisible only with primes dividing $2(P^2+4Q)$.

Now write each one of the factors appearing in the product from the right hand side of formula (84) as

$$\frac{U_{m_i}}{U_{m_{i+1}}} = 2^{\delta_i} D_i F_i \square \quad \text{for } i = 0, 1, \dots, t-1, \tag{89}$$

where $\delta_i \in \{0,1\}$, both D_i and F_i are odd and square-free, $\gcd(P^2+4Q, F_i) = 1$ and D_i is divisible only with primes dividing P^2+4Q. It is clear that every positive integer can be represented in this way and such a representation is unique. From the above arguments, it follows that $\gcd(F_i, F_j) = 1$ for all $i \neq j$. Hence, $\prod_{i=0}^{t-1} F_i$ divides d. All it remains to

notice is that there are at most C_{13} values for $i = 0, \ldots, t-1$ for which $F_i = 1$. Hence,

$$\omega(d) \geq t - C_{13} = \Omega(n) - C_{13}, \tag{90}$$

which is precisely inequality (82).

Proposition 3 is therefore proved. □

We will also need to understand better the prime factors of d appearing in equation (81), when n is divisible with a large power of 2. This is the purpose of the next Proposition.

Proposition 4. *Assume that $n = 2^s m$, where m is odd. Assume that s is much larger than $\omega(n)$. Denote*

$$n_i = 2^i m \quad \text{for } i = 0, 1, \ldots, s \tag{91}$$

and let

$$\frac{U_{n_{i+1}}}{U_{n_i}} = 2^{\delta_i} D_i F_i \square \quad \text{for } i = 0, \ldots, s-1, \tag{92}$$

where $2_i^{\delta} D_i F_i$ is square-free, both D_i and F_i are odd, $D_i \mid P^2 + 4Q$ and F_i is coprime to $P^2 + 4Q$. Then, there exists a computable constant C, such that at least

$$s - \omega(n) - C = \mathrm{ord}_2(n) - \omega(n) - C \tag{93}$$

of the numbers F_i are either divisible with at least two primes, or F_i is a prime $\equiv 3 \pmod 4$.

Proof of Proposition 4. Notice first that the numbers $n_0, n_1, \ldots, n_s$ are precisely the numbers $m_0, m_1, \ldots, m_s$ the only difference being that they are indexed backwards. Thus, the quantities F_i appearing in formula (92) are among the F_i's appearing at the proof of Proposition 3 (to be more precise, the F_i from formula (92) corresponds to F_{s-i} from formula (89)).

By Lemma 3, it follows that at least $s - C_{13}$ of the numbers F_i are not 1. Let us count how many F_i's can be primes congruent to 1 modulo 4. We discard the cases $i = 0$ or 1. For $i \geq 2$, the number

$$\frac{U_{n_{i+1}}}{U_{n_i}} = \frac{U_{2^{i+1}m}}{U_{2^i m}} = V_{2^i m} \tag{94}$$

is a multiple of

$$V_{2^i} = \alpha^{2^i} + \beta^{2^i} = (\alpha^{2^{i-1}} + \beta^{2^{i-1}})^2 - 2(\alpha\beta)^{2^{i-1}} = V_{2^{i-1}}^2 - 2Q^{2^{i-1}}. \tag{95}$$

By formula (95), it follows that V_{2^i} is congruent to 7 modulo 8; hence, with 3 modulo 4. Choose $C_{14} > 1$ such that V_{2^i} is coprime to $P^2 + 4Q$ for all $i > C_{14}$. This can be easily done, since every prime divisor of V_{2^i} is at least as large as $2^{i+1} - 1$. Since $V_{2^i} \equiv 3 \pmod 4$, it follows that $V_{2^i} = d_i \square$, where d_i is square-free, coprime to $P^2 + 4Q$ and is divisible with at least one prime p_i which is 3 modulo 4. Now if F_i is not divisible by p_i, it simply follows that $p_i \mid m$. Notice now that since

$$\gcd(V_{2^i}, V_{2^j}) = 1 \quad \text{for } i \neq j$$

(see [16]), it follows that $p_i \neq p_j$. Hence, there are at most $\omega_0(n) = \omega(m) = \omega(n) - 1$ indices i for which F_i can be a prime congruent to 1 modulo 4. This argument shows that Proposition 4 holds for $C = C_{15} = C_{13} + C_{14}$. □

The situation is not at all as good as illustrated in Propositions 3 and 4 when U_n is replaced by V_n in equation (81). However, the following result turns out to be helpful.

Proposition 5. *Let $n = 2^s m$, where m is odd. There exists a computable constant C, such that if*

$$V_n = d \square, \tag{96}$$

then

$$\Omega(m) \leq \omega(d) + C + \omega(V_{2^s}). \tag{97}$$

Proof of Proposition 5. The proof of Proposition 5 is similar to the proof of Proposition 3. We shall just sketch it here to make clear why we needed to add the extra term $\omega(V_{2^s})$ at the right hand side of inequality (97).

Let $t = \Omega(m)$ and assume that $q_1 \leq q_2 \leq \cdots \leq q_t$ are all the primes (counted with multiplicities) dividing m. Denote $m_0 = n = 2^s m$ and

$$m_i = \frac{n}{q_1 \dots q_i} = 2^s q_{i+1} \dots q_t \quad \text{for } i = 1, \dots, t. \tag{98}$$

Write equation (96) as

$$d\square = V_n = \frac{V_{m_0}}{V_{m_1}} \cdot \frac{V_{m_1}}{V_{m_2}} \cdot \ldots \cdot \frac{V_{m_{t-1}}}{V_{m_t}} \cdot V_{2^s}. \tag{99}$$

One can show, as in the proof of Proposition 3, that the greatest common divisor of any two of the numbers

$$\frac{V_{m_i}}{V_{m_{i+1}}} \quad \text{for } i = 0, 1, \ldots, t \tag{100}$$

is divisible only with primes dividing $2(P^2 + 4Q)V_{2^s}$. Hence, if one writes

$$\frac{V_{m_i}}{V_{m_{i+1}}} = 2^{\delta_i} D_i F_i \square \quad \text{for } i = 0, 1, \ldots, t-1, \tag{101}$$

where $2^{\delta_i} D_i F_i$ is square-free, both D_i and F_i are odd, F_i is coprime to $P^2 + 4Q$ and D_i is divisible only with primes dividing $P^2 + 4Q$, it then follows, by Lemma 3, that there are at most C_{13} indices i for which F_i is 1. Hence, there are at least $\Omega(m) - C_{13}$ such indices i for which F_i is not 1. However, it could happen that $F_i \mid V_{2^s}$. At any rate, since $\gcd(F_i,\ F_j) = 1$ for $i \neq j$, it follows that $F_i \mid V_{2^s}$ in at most $\omega(V_{2^s})$ instances. Hence,

$$\Omega(m) - C_{13} - \omega(V_{2^s}) \leq \omega(d), \tag{102}$$

which is precisely inequality (97) with $C = C_{13}$.

We conclude here our analyzis of $\Omega(n)$ in terms of $\omega(d)$ where d is the square-free part of W_n. □

5. The proof of the Theorem

Assume that

$$\sigma(W_n) = kW_n \tag{103}$$

for some n and k. We shall exploit the order at which 2 can appear in the right hand side of equation (103). We need the following lemma.

Lemma 4. *Assume that $n = 2^s m$, where $m \geq 1$ is odd. Then, there exists a constant C, such that*

$$\operatorname{ord}_2(W_n) \leq \begin{cases} C + s & \text{if } W_n = U_n, \\ C & \text{if } W_n = V_n. \end{cases} \tag{104}$$

Proof of Lemma 4. This is well-known. One can take

$$C = C_{16} = \max(\operatorname{ord}_2(U_3), \operatorname{ord}_2(U_6), \operatorname{ord}_2(V_3), \operatorname{ord}_2(V_6)). \tag{105}$$ □

We begin by bounding $\Omega(n)$, k and $q(n)$.

Case I. $W_n = U_n$.

Write

$$\sigma(U_n) = kU_n. \tag{106}$$

By Lemma 4, it follows that

$$\begin{aligned} \operatorname{ord}_2(\sigma(U_n)) &= \operatorname{ord}_2(kU_n) = \operatorname{ord}_2(k) + \operatorname{ord}_2(U_n) \\ &\leq \log_2 k + s + C_{16}. \end{aligned} \tag{107}$$

Now write

$$U_n = d\,\square. \tag{108}$$

By formula (107), it follows that

$$\omega(d) \leq \operatorname{ord}_2(\sigma(U_n)) + 1 \leq \log_2 k + s + C_{17}, \tag{109}$$

where $C_{17} = C_{16} + 1$. By inequalities (90) and (109), we get

$$\Omega(n) \leq \omega(d) + C_{13} \leq \log_2 k + s + C_{18}, \tag{110}$$

where $C_{18} = C_{13} + C_{17}$. Since $\Omega(n) = s + \Omega(m) \geq s + \omega(n) - 1$, we get

$$\omega(n) \leq \Omega(n) - s + 1 \leq \log_2 k + C_{18} + 1$$

or

$$\omega(n) \log 2 \leq \log k + C_{19}, \tag{111}$$

where $C_{19} = (C_{18} + 1) \log 2$. On the other hand, since

$$\log k = \log \left(\frac{\sigma(U_n)}{U_n} \right), \tag{112}$$

it follows, by inequalities (33) and (111), that

$$\omega(n) \log 2 < u_n + C_{19} + C_7 \log^2(\omega(n) + 1), \tag{113}$$

where u_n is given by formula (21). Since u_n is bounded by C_3, inequality (113) implies that $\omega(n) < C_{20}$. From equation (112), inequality (33) and the fact that $\omega(n) < C_{20}$, we get

$$\begin{aligned} \log k = \log \left(\frac{\sigma(U_n)}{U_n} \right) &< u_n + C_7 \log^2(\omega(n) + 1) \\ &< C_3 + C_7 \log^2(C_{20}^2 + 1) = C_{21}. \end{aligned} \tag{114}$$

Hence, k is bounded as well. We now bound $q(n)$. If $q(n) \leq C_1$, there is nothing to bound. So, we assume that $q(n) > C_1$. In this case, formula (21), inequality (29) and equation (112), give

$$\log k < 4 \left(\sum_{q|n} \frac{\log q}{q-1} \right) \prod_{q|n} \left(1 + \frac{1}{q-1} \right). \tag{115}$$

Since $k \geq 2$ and $\omega(n) < C_{20}$, inequality (115) implies

$$\begin{aligned} \log 2 &< 4 \frac{\omega(n) \log q(n)}{q(n)-1} \left(1 + \frac{1}{q(n)-1} \right)^{\omega(n)} \\ &< \frac{4 C_{20} \log q(n)}{q(n)-1} \left(1 + \frac{1}{q(n)-1} \right)^{C_{20}}. \end{aligned} \tag{116}$$

Notice that the function of $q(n)$ appearing in the right hand side of inequality (116) tends to zero when $q(n)$ is large. Hence, inequality (116) implies that $q(n) < C_{22}$.

It remains to bound $\Omega(n)$. We start by bounding s. By Proposition 4, we know that for s large, the square-free number d appearing in the right hand side of equation (108) has at least $s - \omega(n) - C_{15}$ odd coprime factors of the form F_i, such that each one of these factors is either a product of two

(or more) distinct primes, or is a prime congruent to 3 modulo 4. Notice that each one of these factors F_i will bring a contribution of at least 2 in $\mathrm{ord}_2(d)$; hence in $\mathrm{ord}_2(\sigma(U_n))$. These arguments combined with inequality (107), show that

$$2(s - \omega(n) - C_{16}) \leq \log_2 k + s + C_{16}$$

or

$$s < \log_2 k + 2\omega(n) + 2C_{16} + C_{17} < C_{23}, \tag{117}$$

because both k and $\omega(n)$ have already been bounded. Finally, notice that inequality (110) together with the fact that both s and k are bounded leads to the conclusion that $\Omega(n)$ is bounded as well.

Case II. $W_n = V_n$.

Write

$$\sigma(V_n) = kV_n. \tag{118}$$

By Lemma 4, it follows that

$$\mathrm{ord}_2(\sigma(V_n)) = \mathrm{ord}_2(kV_n) = \mathrm{ord}_2(k) + \mathrm{ord}_2(V_n) \leq \log_2 k + C_{16}. \tag{119}$$

Now write

$$V_n = d\,\square. \tag{120}$$

By formula (120) and inequality (119), it follows that

$$\omega(d) \leq \mathrm{ord}_2(\sigma(V_n)) + 1 \leq \log_2 k + C_{17}. \tag{121}$$

By inequalities (102) and (121), we get

$$\Omega(m) \leq \omega(d) + C_{17} + \omega(V_{2^s}) \leq \log_2 k + C_{24} + \omega(V_{2^s}), \tag{122}$$

where $C_{24} = C_{17} + C_{13}$. Since

$$V_{2^s} = \alpha^{2^s} + \beta^{2^s},$$

it follows that

$$\omega(V_{2^s}) < 2^s C_{25}, \tag{123}$$

where $C_{25} = \log|\alpha| + 1$. Inequality (122), together with the fact that $\omega(n) \le \Omega(m) + 1$, imply

$$\omega(n) \le \log_2 k + C_{24} + 1 + 2^s C_{25}. \tag{124}$$

We now find bounds on s, k and $\Omega(n)$. Assume first that $s > C_9$ and we shall return to the case when $s \le C_9$ later.

Since

$$\log k = \log\left(\frac{\sigma(V_n)}{V_n}\right), \tag{125}$$

it follows, by formula (125) and inequality (46), that

$$\log k < \frac{1}{1.5^s}\left(C_8 v'_m + C_{12}\log^2(\omega(m)+1)\right) \quad \text{for } s > C_9, \tag{126}$$

where $v'_m < C_3$. Inequalities (124) and (126) give

$$\log k < \frac{1}{1.5^s}\left(C_8 \cdot C_3 + C_{12}\log^2\left(\log_2 k + C_{24} + 2 + 2^s C_{25}\right)\right)$$
$$\text{for } s > C_9. \tag{127}$$

It is not that hard to see that inequality (127) forces that both k and s are bounded by C_{26}. Inequalities (122) and (123) imply now that $\Omega(m)$ is bounded; hence $\Omega(n) = \Omega(m) + s$ is bounded as well.

However, notice that the previous arguments were done assuming that $s > C_9$. We still need to justify that both k and $\Omega(n)$ are bounded even when $s \le C_9$. But assume that $s \le C_9$. Inequality (124) implies that

$$\omega(n) \le \log_2 k + C_{27}. \tag{128}$$

Combining inequality (35), formula (125) and inequality (128), we get

$$\log k < v_n + C_7\log^2(\omega(n)+1) < C_3 + C_7\log^2(\log_2 k + C_{27}). \tag{129}$$

Inequality (129) implies that k is bounded and then inequality (122) implies that $\Omega(m)$ is bounded; hence $\Omega(n) = \Omega(m) + s$ is bounded as well.

We need to show that $q(n)$ is bounded as well. If $q(n) \leq C_1$, then certainly $q(n)$ is bounded. When $q(n) > C_1$, formulae (34) and (125) imply that

$$\begin{aligned} \log k &< 4 \left(\sum_{q|n} \frac{\log q}{q-1} \right) \prod_{q|n} \left(1 + \frac{1}{q-1} \right) \\ &< 4 \frac{\omega(n) \log q(n)}{q(n)-1} \left(1 + \frac{1}{q(n)-1} \right)^{\omega(n)} . \end{aligned} \tag{130}$$

Since $k \geq 2$ and $\omega(n)$ is bounded, inequality (130) implies that $q(n)$ is bounded as well.

Hence, we have showed that in both instances there exists a bound C_{28} such that

$$\max(\Omega(n), q(n), k) < C_{28}. \tag{131}$$

Assume also that $C_{28} > 2$ is larger than the largest prime dividing P^2+4Q. Finally, set $C = C_{28}$.

We now proceed to give the closing argument.

Assume that C is an integer (if not, just round it up to the next integer).

For any subset $\mathcal{P}$ of primes, denote by

$$\mathrm{Cl}\,\mathcal{P} = \{q \mid q \leq p \text{ for some } p \in \mathcal{P}\}\,. \tag{132}$$

That is, Cl stands for the closure operator with respect to the $\leq$ order restricted only to subsets consisting of primes.

We assume first that $(W_n)_{n\geq 0} = (U_n)_{n\geq 0}$. Let

$$A_1 = \{q \mid q < C\} \tag{133}$$

and

$$B_1 = A_1. \tag{134}$$

Assume that $i \geq 1$ and that both A_i and B_i have been constructed. Let

$$\begin{aligned} A_{i+1} = A_i &\cup \mathrm{Cl}\left\{q \mid q \,|\, U_m \text{ for some } m \in B_i\right\} \\ &\cup \mathrm{Cl}\left\{q \mid q \,|\, r(r^2-1) \text{ for some prime } r \text{ such that } r \mid \sigma(U_m) \text{ for some } m \in B_i\right\} \end{aligned} \tag{135}$$

and

$$B_{i+1} = \{m \mid m = q_1 q_2 \dots q_t \text{ for some } t \le i+1 \text{ and } p_j \in A_i \text{ for all } j = 1, \dots, t\}. \tag{136}$$

We also assume that $1 \in A_1$.

In this case, the proof ends once we prove the following:

Lemma 5. *If U_n is multiply perfect, then $n \in B_C$.*

Proof of Lemma 5. Assume that U_n is multiply perfect and let $q_1 \le q_2 \le \cdots \le q_t$ be all the prime divisors (counted with multiplicities) of n. Since $t = \Omega(n) < C$, it suffices to prove that $q_i \in A_i$. This can be easily done by induction. We outline only the induction step for $i = 2$.

Clearly, $q_1 = q(n) \in A_1$. If $n = q_1$, we are done. Assume now that $n > q_1$. Write

$$U_n = U_{q_1} \cdot \frac{U_n}{U_{q_1}}. \tag{137}$$

If the two factors of the product appearing in the right hand side of equality (137) are not coprime, it simply follows that there exists a prime $q_j \mid n$ with $j \ge 2$, such that $q_j \mid U_{q_1}$. In particular, $q_j \in A_2$. Since A_2 is closed to the left, it follows that $q_2 \in A_2$.

Assume now that the two factors appearing in the right hand side of formula (137) are coprime. Then,

$$\sigma(U_n) = \sigma(U_{q_1}) \cdot \sigma\left(\frac{U_n}{U_{q_1}}\right) = kU_n = kU_{q_1} \cdot \frac{U_n}{U_{q_1}}. \tag{138}$$

Assume first that

$$\gcd\left(\sigma(U_{q_1}), \frac{U_n}{U_{q_1}}\right) \ne 1. \tag{139}$$

Let r be a prime divisor of the greatest common denominator appearing in formula (139). In particular, $r \mid \sigma(U_{q_1})$ and $r \mid U_n$. Since $r \mid U_{r(r^2-1)}$, it follows that

$$r \mid \gcd(U_n, U_{r(r^2-1)}) = U_{(r(r^2-1),n)}. \tag{140}$$

Formula (140) shows that $q_j \mid r(r^2-1)$ for some $j \geq 1$. If $j > 1$, it follows that $q_j \in A_2$, therefore $q_2 \in A_2$ as well. If $j = 1$, it follows that $r \mid U_{q_1}$. Hence,

$$r \mid \gcd\left(\frac{U_n}{U_{q_1}}, U_{q_1}\right), \tag{141}$$

which is impossible since we assumed that the two numbers above are coprime.

Finally, assume that $\sigma(U_{q_1})$ and U_n/U_{q_1} are coprime. From equation (138), it follows that $\sigma(U_{q_1}) \mid kU_{q_1}$. Denoting by k_1 the ratio of kU_{q_1} to $\sigma(U_{q_1})$, we get

$$\sigma\left(\frac{U_n}{U_{q_1}}\right) = k_1 \frac{U_n}{U_{q_1}}. \tag{142}$$

In particular, U_n/U_{q_1} is multiply perfect. From the above arguments, it follows easily that $q_2 \in A_1$. Indeed, this follows, for example, from the way the upper bound C on $q(n)$ was chosen (see inequality (130)). Hence, $q_2 \in A_1 \subseteq A_2$.

The general induction step follows from similar arguments. We do not give further details. □

We finally treat the case $(W_n)_{n\geq 0} = (V_n)_{n\geq 0}$. Fix $s \geq 0$. Set

$$A_1^s = \{q \mid q < C\} \cup \mathrm{Cl}\left\{q \;\middle|\; q \mid V_{2^s}\right\} \tag{143}$$

and

$$B_1^s = \{2^s q \mid \text{for some odd } q \in A_1^s\}. \tag{144}$$

Let $i \geq 1$ and assume that A_i^s and B_i^s have been constructed. Set

$$\begin{aligned} A_{i+1}^s = A_i^s &\cup \mathrm{Cl}\left\{q \mid q \,|\, V_m \text{ for some } m \in B_i^s\right\} \\ &\cup \mathrm{Cl}\left\{q \mid q \,|\, r(r^2-1) \text{ for some } r \text{ prime where } r \,|\, \sigma(V_m) \text{ for some } m \in B_i^s\right\} \end{aligned} \tag{145}$$

and

$$B_{i+1}^s = B_i^s \cup \left\{m \mid m = m_1 q \text{ for some } m_1 \in B_i^s \text{ and some odd } q \in A_{i+1}^s\right\}. \tag{146}$$

We assume again that $1 \in A_1^s$ for all $s \geq 0$.

Then, the claim is:

Lemma 6. *If V_n is multiply perfect, then*

$$n \in \bigcup_{s=0}^{C-1} B^s_{C-s}. \tag{147}$$

Proof of Lemma 6. Follows from arguments similar to the ones employed at the proof of Lemma 5. The only reason why we needed to separate the powers of 2, was to insure that the inductive argument applied in the proof of Lemma 4, which was based on the idea of reducing the problem for W_{mq} to the problem for $W_{mq}/W_q = W'_m$, can still be applied.

The Theorem is therefore proved. □

Remark. One can see from the above algorithm why the size of the computable constant C such that $n < C$, whenever W_n is multiply perfect, can be as large as claimed in Section 2.

References

[1] Y. Bilu, G. Hanrot and P. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, (*preprint* 1999).

[2] R. D. Carmichel, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913–1914), 30–70.

[3] J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537–540.

[4] J. H. E. Cohn, Squares in some recurrent sequences, *Pacific J. of Math.* **41** (1972), 631–648.

[5] H. Harborth, Perfect number pairs, Proceedings of the Eight International Conference on Fibonacci numbers and their Applications, Rochester, June, 1998 (*to appear*).

[6] F. Luca, Euler indicators of Lucas sequences, *Bull. Mat. Soc. St. Mat. Roumanie* **88** (1997), 151–163.

[7] F. Luca, On the equation $\phi(x^m - y^m) = x^n + y^n$, *Bull. Irish Math. Soc.* **40** (1998), 46–55.

[8] F. Luca, On the equation $\phi(|x^m + y^m|) = |x^n + y^n|$, *Indian J. of P. App. Math.* **30**(2) (1999), 183–197.

[9] F. Luca, Arithmetic functions of Fibonacci numbers, *Fibo. Quart.* **37** (1999), 265–268.

[10] F. Luca, Equations involving arithmetic functions of Fibonacci and Lucas numbers (*to appear in* Fibo. Quart.).

[11] F. Luca, On the equation $\phi(|x^m - y^m|) = 2^n$ (*to appear in* Math. Bohemica).

[12] F. Luca, Euler indicators of binary recurrence sequences, (*submited*).

[13] F. Luca, Perfect Fibonacci and Lucas numbers (*to appear in* Rend. Circolo Math. Palermo).

[14] F. Luca, Amicable Pell numbers, (*submited*).

[15] D. W. Masser, How to solve a quadratic equation in rationals, *Bull. London Math. Soc.* **30** (1998), 24–28.

[16] W. L. McDaniel, The g.c.d. in Lucas sequences and Lehmer number sequences, *Fibo. Quart.* **29** (1991), 24–29.

[17] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* **15** (1982), 5–13.

[18] P. Ribenboim, Square classes of Fibonacci and Lucas numbers, *Port. Math.* **46** (1989), 159–175.

[19] P. Ribenboim, Square classes of $\frac{a^n-1}{a-1}$ and a^n+1, *J. Sichuan Univ.* **26** (1989), 196–199.

[20] P. Ribenboim and W. L. McDaniel, Square classes of Lucas sequences, *Port. Math.* **48** (1991), 469–473.

[21] P. Ribenboim and W. L. McDaniel, The square terms in Lucas sequences, *J. Number Theory* **58** (1996), 104–122.

[22] P. Ribenboim and W. L. McDaniel, Square classes in Lucas sequences having odd parameters, *J. Number Theory* **73** (1998), 14–27.

[23] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. of Math.* **6** (1962), 64–94.

[24] A. Rotkiewicz, Applications of Jacobi's symbol to Lehmer's numbers, *Acta Arith.* **42** (1983), 163–187.

[25] T. N. Shorey and C. L. Stewart, On the diophantine equation $ax^{2n}+bx^ny+cy^2=d$ and pure powers in recurrence sequences, *Math. Scand.* **52** (1983), 24–36.

[26] T. N. Shorey and R. Tijdeman, Exponential Diophantine Equations, *Cambridge University Press*, *Cambridge*, 1986.

FLORIAN LUCA
MATHEMATICAL INSTITUTE
CZECH ACADEMY OF SCIENCES
ŽÍTNA 25
115 67 PRAHA 1
CZECH REPUBLIC

E-mail: luca@matsrv.math.cas.cz

(Received May 26, 1999; revised November 16, 1999)