LUCAS SEQUENCES FOR WHICH $4 \mid \phi(|u_n|)$ FOR ALMOST ALL n

Florian Luca
Instituto de Matemáticas de la UNAM, Campus Morelia, Apartado Postal 61-3
(Xangari) CP58089 Morelia, Michoacán, Mexico
e-mail: fluca@matmor.unam.mx

Lawrence Somer
Department of Mathematics, Catholic University of America, Washington, D.C. 20064
e-mail: somer@cua.edu

(Submitted October 2004-Final Revision May 2005)

ABSTRACT

In this paper, we look at those pairs of integers (a, b) for which the Lucas sequence of general term $u_n = u_n(a, b)$ has the property that $4 \mid \phi(|u_n|)$ for almost all positive integers n.

1. INTRODUCTION

In a brilliant short solution (certainly one included in Erdős's Book of ideal proofs) to a problem proposed by Clark Kimberling [9] in 1976, Peter Montgomery [15] showed that $4 \mid \phi(F_n)$ for all $n > 4$, where $\phi(n)$ denotes Euler's totient function. This problem was originally proposed by Douglas Lind [12] in this Quarterly in 1965 and given an incomplete solution by John L. Brown, Jr. [2]. For another solution of this problem, see [8].

In [14], Wayne McDaniel proved the following two theorems:

Theorem 1.1: *If $n \neq 1, 2, 3, 4, 6, 8, 12, 16, 24, 32,$ or 48, then F_n has at least one prime factor of the form $4r + 1$.*

Theorem 1.2: *Let P_n denote the n^{th} Pell number ($P_{n+2} = 2P_{n+1} + P_n,\ P_0 = 0,\ P_1 = 1$). If $n \neq 1, 2,$ or 4, then P_n has at least one prime factor of the form $4r + 1$.*

Remark 1.3: *In Theorem 1.1, McDaniel left out the case $F_{12} = 144 = 2^4 3^2$, while in Theorem 1.2, McDaniel inadvertently included the case $P_{14} = 80782 = 2 \cdot 13^2 \cdot 239$.*

The problems considered by Montgomery and McDaniel are related in that if a positive integer n has a prime factor $p \equiv 1 \pmod 4$, then $4 \mid \phi(n)$. In this paper, we will generalize both Montgomery's and McDaniel's results to infinite classes of Lucas sequences, classes which cover *most* Lucas sequences.

2. PRELIMINARIES

Before presenting our main theorems, we will need to introduce some definitions and notation and give some known results. We also prove Lemma 2.21, which will be needed for the proofs of our main theorems.

Let $u(a, b)$ and $v(a, b)$ be Lucas sequences satisfying the second-order recursion relation

$$w_{n+2}(a, b) = aw_{n+1}(a, b) + bw_n(a, b), \tag{2.1}$$

where a and b are integers, and the initial terms are $u_0 = 0, u_1 = 1$ and $v_0 = 2, v_1 = a$, respectively. Associated with $u(a, b)$ and $v(a, b)$ is the characteristic polynomial

$$f(x) = x^2 - ax - b \tag{2.2}$$

with characteristic roots α and β. Let $D = D(a,b) = (\alpha - \beta)^2 = a^2 + 4b$ be the discriminant of both $u(a,b)$ and $v(a,b)$. By the Binet formulas,

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad v_n = \alpha^n + \beta^n \tag{2.3}$$

if $D \neq 0$ and

$$u_n = n\alpha^{n-1} = n(a/2)^{n-1},\ v_n = 2\alpha^n = 2(a/2)^n \tag{2.4}$$

if $D = 0$. Note that by (2.3) and (2.4), $u_m | u_n$ if $m|n$.

The rank of appearance of the positive integer m in $u(a,b)$ (respectively, in $v(a,b)$), denoted by $\rho(m)$ (respectively, $\overline{\rho}(m)$), is the least positive integer t such that $m|u_t$ (respectively, $m|v_t$). Since $u_0 = 0$, it is easily seen that $\rho(m)$ exists if $gcd(m,b) = 1$. The prime p is called a primitive prime divisor of u_n if $p|u_n$, but $p \not| u_k$ for $1 \leq k < n$. A primitive prime divisor of v_n is defined similarly. It is known that if p is primitive for either u_n or v_n, then $p \equiv \pm 1 \pmod{n}$, except when $p \mid D$, case in which $p \mid u_p$. In particular, $p \geq n - 1$.

The Lucas sequences $u(a,b)$ and $v(a,b)$ are called degenerate if either $ab = 0$ or α/β is a root of unity. Since the characteristic polynomial f of $u(a,b)$ and $v(a,b)$ is a quadratic polynomial with integer coefficients, one sees that α/β can be a primitive root of unity only if $n = 1,\ 2,\ 3,\ 4,$ or 6. The following theorem gives all degenerate Lucas sequences $u(a,b)$ and $v(a,b)$.

Theorem 2.1: *Let N denote an arbitrary nonzero integer. Then the Lucas sequences $u(a,b)$ and $v(a,b)$ with characteristic roots α and β are degenerate only in the following cases:*

(i) $b = 0$, *a is any integer. Then* $D = a^2,\ u_n = a^{n-1}$, *and* $v_n = a^n$ *for* $n \geq 1$.

(ii) $\alpha/\beta = 1$. *Then* $a = 2N,\ b = -N^2$, *and* $D = 0$.

(iii) $\alpha/\beta = -1$. *Then* $a = 0,\ b = -N$, *and* $D = 4N$.

(iv) α/β *is a primitive cube root of unity. Then* $a = N,\ b = -N^2$, *and* $D = -3N^2$.

(v) α/β *is a primitive fourth root of unity. Then* $a = 2N,\ b = -2N^2$, *and* $D = -4N^2$.

(vi) α/β *is a primitive sixth root of unity. Then* $a = 3N,\ b = -3N^2$, *and* $D = -3N^2$.

Proof: This is proved in [24, p. 613]. □

The proposition below gives well-known properties of the Euler phi-function, which will be needed for our further work (see [3, pp. 129-132]). The phi-function ϕ is only defined for positive integers n. We recall that for a positive integer n the number $\phi(n)$ counts the number of positive integers $m \leq n$ which are coprime to n.

Proposition 2.2: *Let m and n be positive integers.*

(i) If $gcd(m,n) = 1$, *then* $\phi(mn) = \phi(m)\phi(n)$.

(ii) If

$$n = \prod_{i=1}^{r} p_i^{k_i}$$

is the prime power factorization of n, then

$$\phi(n) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1).$$

(iii) If $m|n$, then $\phi(m)|\phi(n)$.

The following two lemmas will be key tools in proving that $4 \mid \phi(|u_n|)$ in various cases.

Lemma 2.3: *Let $u(a,b)$ be a nondegenerate Lucas sequence for which $gcd(a,b) = 1$.*
(i) If $m|n$ and $4 \mid \phi(|u_m|)$, then $4 \mid \phi(|u_n|)$.
(ii) Suppose that $n > 3$, u_n has a primitive prime divisor p, and there exists a positive integer $m > 1$ such that $m|n$, $m \neq n$, and $|u_m| \geq 3$. Then $4 \mid \phi(|u_n|)$.

Proof:
(i) This follows from Proposition 2.2 (iii) since $m|n$ implies that $u_m|u_n$.
(ii) Since $n > 3$, and p is primitive for u_n, it follows that $p \geq n - 1 \geq 3$. Note that $pu_m|u_n$ and $gcd(p, u_m) = 1$. It now follows from Proposition 2.2 that $4 \mid \phi(|pu_m|)$ and hence, $4 \mid \phi(|u_n|)$. □

Lemma 2.4: *Let n be a positive integer. Then $4 \not| \phi(n)$ if and only if $n = 1,\ 2,\ 4,\ p^k$, or $2p^k$, where p is a prime congruent to $3 \pmod 4$ and $k \geq 1$.*

Proof: This follows from Proposition 2.2 (ii). □

Lemma 2.5:

$$u_n(-a,b) = (-1)^{n+1}u_n(a,b). \tag{2.5}$$

$$v_n(-a,b) = (-1)^n v_n(a,b). \tag{2.6}$$

Proof: Equations (2.5) and (2.6) follow from the Binet formulas (2.3) and (2.4) and can be proved by induction. □

Remark 2.6: *In all the proofs from here on, we will only be concerned with the absolute values of $u_n(a,b)$ and $v_n(a,b)$. Accordingly, by virtue of equations (2.5) and (2.6), we will assume that $a > 0$ in all our subsequent proofs involving $u_n(a,b)$ and $v_n(a,b)$.*

Proposition 2.7: *Let $u(a,b)$ and $v(a,b)$ be Lucas sequences for which $gcd(a,b) = 1$. Then the following hold:*
(i) $gcd(u_n, b) = gcd(v_n, b) = 1$ for $n \geq 1$.
(ii) $gcd(u_n, v_n) = 1$ or 2 for $n \geq 1$.
(iii) $gcd(u_m, u_n) = |u_d|$, where $d = gcd(m,n)$.

Proof: Part (i) is proved in Theorem I of [4], part of (ii) is proved in Theorem II of [4], and part (iii) is proved in Theorem VI of [4]. □

Lemma 2.8: *Let $u(a,b)$ and $v(a,b)$ be Lucas sequences such that $ab \neq 0$ and $D = a^2 + 4b > 0$. Then $|u_n|$ is strictly increasing for $n \geq 2$ and $|v_n|$ is strictly increasing for $n \geq 1$. Further, if $a > 0$, then $u_n > 0$ for $n \geq 1$. Moreover, if $b \leq -1$, then $|a| \geq 3$, $|u_{n+1}| > |(a/2)u_n|$, and $|v_{n+1}| > |(a/2)v_n|$ for $n \geq 1$. Furthermore, if it is not the case that $|a| = b = 1$, then $|u_3| \geq 3$.*

Proof: In light of Remark 2.6, we may assume that $a \geq 1$. Each assertion except the last one is proved in the proof of Lemma 3 in [7]. To prove the last assertion, we first observe that if $b \geq 1$ and it is not the case that $a = b = 1$, then clearly $u_3 = a^2 + b \geq 3$. If $b \leq -1$, then $a \geq 3$ and $u_3 > (3/2)u_2 = 3a/2 \geq 9/2$. □

Remark 2.9: *By Remark 2.6 and Lemma 2.8, we can assume in our proofs from here on that if $D > 0$, then $u_n > 0$ for $n \geq 1$.*

Lemma 2.10: *Let $u(a,b)$ and $v(a,b)$ be Lucas sequences for which $2 \not| gcd(a,b)$.*
(i) Suppose a is odd and b is even. Then $2 \not| u_n$ and $2 \not| v_n$ for $n \geq 1$.
(ii) Suppose a is even and b is odd. Then $2|u_n$ if and only if $2|n$, and $2|v_n$ for all $n \geq 0$.

(iii) *Suppose a and b are both odd. Then $2|u_n$ if and only if $3|n$, and $2|v_n$ if and only if $3|n$. Moreover, $8|u_6$.*
(iv) *If $\rho(2)$ exists, then $\rho(2) \leq 3$.*
(v) *If $\overline{\rho}(2)$ exists, then $\overline{\rho}(2) \leq 3$.*

Proof: Parts (iv) and (v) follow from parts (i) - (iii). All the rest of the assertions except the last assertion of parts (i) - (iii) are proved in [16, p. 60]. We now prove that if $a \equiv b \equiv 1 \pmod 2$, then $8|u_6$. Note that $u_6 = u_3 v_3 = (a^2+b)(a(a^2+3b))$. Then $2|a^2+b$ and $2|a^2+3b$. Moreover, $4|a^2+b$ or $4|a^2+3b$, depending on whether $b \equiv 3 \pmod 4$ or $b \equiv 1 \pmod 4$), respectively. Thus, $8|u_6$. □

Proposition 2.11: *Let $u(a,b)$ be a Lucas sequence.*
(i) $u_n^2 - u_{n-1}u_{n+1} = (-b)^{n-1}$.
(ii) $u_{2n+1} = bu_n^2 + u_{n+1}^2$.

Proof: Parts (i) and (ii) follow from the Binet formulas (2.3) and (2.4). □

Lemma 2.12: *Let $u(a,b)$ be a Lucas sequence for which $gcd(a,b) = d > 1$. Then $d^k|u_n$ for $n \geq 2k$, where $k \geq 1$.*

Proof: This follows easily by induction using the recursion relation defining $u(a,b)$. □

Theorems 2.13, 2.14, 2.16, 2.17, and 2.18 below, dealing with primitive prime divisors of u_n and with determining when $|u_n|$ can be a square, will play primary roles in showing that $4 \mid \phi(|u_n|)$.

Theorem 2.13: *Let $u(a,b)$ be a Lucas sequence for which $gcd(a,b) = 1$, $ab \neq 0$, and $D > 0$. Then u_n has a primitive prime divisor unless n=1, 2, 6, or 12. Moreover, $u_{12}(a,b)$ has no primitive prime divisor if and only if $|a| = b = 1$.*

Proof: This is proved in Theorem XXIII of [4]. □

Theorem 2.14: *Let $u(a,b)$ be a nondegenerate Lucas sequence for which $gcd(a,b) = 1$. Then u_n has a primitive prime divisor if $n > 30$. Moreover, u_n also has a primitive prime divisor unless n=1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 18, or 30.*

Proof: This is proved in Theorems C, 1.3, and 1.4 of [1]. □

Remark 2.15: *Consider all nondegenerate Lucas sequences $u(a,b)$ for which $gcd(a,b) = 1$. Tables 1 and 3 of [1] list all terms $u_n(a,b)$, $n \geq 1$, which have no primitive prime divisors. We note that in [1], the authors define a prime p to be a primitive prime divisor of u_n if $p|u_n$ but $p \not| Du_1u_2 \ldots u_{n-1}$. In contrast to this definition, we include p as a primitive prime divisor of u_n if $p|D$ but $p \not| u_k$ for $1 \leq k < n$.*

Theorem 2.16: *Let the Lucas sequence $u(a,b)$ be nondegenerate. Then there exists a constant $N_1(a,b)$ dependent on a and b such that $u_n(a,b)$ has an odd primitive prime divisor for all $n > N_1(a,b)$.*

Proof: This was proved by Lekkerkerker [11] for the case in which $D > 0$ and by Schinzel [20] for the case in which $D < 0$. In fact, the argument from page 74 in [23] together with the main result of [1] shows that one may choose $N_1(a,b) = \max\{P(b)+1, 30\}$, where $P(b)$ denotes the largest prime factor of b with the convention that $P(\pm 1) = 1$. □

Theorem 2.17: *Let $u(a,b)$ be a nondegenerate Lucas sequence for which $-b$ is a square and $gcd(a,b) = 1$.*
(i) If $D > 0$, then $u_n(a,b)$ has two odd primitive prime divisors for $n > 3$ an odd integer.
(ii) If $D < 0$, then there exists a constant $N_2(a,b)$ dependent on a and b such that if n is odd and $n > N_2(a,b)$, then $u_n(a,b)$ has two odd primitive prime divisors.

Proof: Part (i) is proved in [19] and [21] and part (ii) is proved in [21]. □

Remark 2.18: *In part (i) of Theorem 2.17, both the papers [19] and [21] exclude the case in which* $a = 3$ *and* $b = -1$. *However* $u_5(3, -1) = 55 = 5 \cdot 11$, *and according to our definition it has two odd primitive prime divisors.*

Theorem 2.19:

(i) $u_3(1, 1) = 2$ *and* $u_6(1, 1) = 8$ *are the only Fibonacci numbers* F_n *which are twice a square for* $n > 1$.

(ii) $|u_4(\pm 8, -7)| = 20^2$ *and* $|u_5(\pm 4, -3)| = 11^2$ *are the only instances in which* $|u_n(a, b)|$ *is a square when* $n > 2,\ b < -1$, *and* $|a| = -b + 1$.

(iii) Let $n \geq 1$ *and let* $u(a, b)$ *be a Lucas sequence for which* $a \equiv b \equiv 1 \pmod 2$, $gcd(a, b) = 1$, *and* $D > 0$. *Then* $|u_n(a, b)|$ *can be a square only if n=1, 2, 3, 6, or 12.*

(iv) Let $u(a, b)$ *be a nondegenerate Lucas sequence for which* $gcd(a, b) = 1$. *Then there exists an effectively computable constant* $N_3(a, b)$, *dependent on a and b, such that* $|u_n(a, b)|$ *is not a square if* $n > N_3(a, b)$.

Proof: Part (i) is proved in [5] and [6], (ii) is proved in [13], (iii) is proved in [18], and (iv) is proved in [16] and [22]. A generalization of (iv) is proved in Chapter 9 of [23]. □

Lemma 2.20: *Let* $v(a_1, b_1)$ *be a nondegenerate Lucas sequence for which* $gcd(a_1, b_1) = 1$. *Let* $k \geq 2$ *and let* $a = v_k(a_1, b_1)$ *and* $b = (-1)^{k+1} b_1^k$. *Then* $u(a, b)$ *is a nondegenerate Lucas sequence for which*

$$u_n(a, b) = \frac{u_{kn}(a_1, b_1)}{u_k(a_1, b_1)}, \tag{2.7}$$

$gcd(a, b) = 1$, *and both* $D = D(a, b)$ *and* $D_1 = D(a_1, b_1)$ *have the same sign.*

Proof: Suppose that $u(a_1, b_1)$ has the characteristic roots α and β. It was shown in [10, p. 437] that (2.7) holds, the characteristic roots of $u(a, b)$ are α^k and β^k, and $D = D_1 u_k^1(a_1, b_1)$. Hence, D and D_1 have the same sign and $u(a, b)$ is nondegenerate. Since $gcd(v_k(a_1, b_1), b_1) = 1$ by Proposition 2.7 (i), it follows that $gcd(a, b) = 1$. □

Lemma 2.21: *Let* $u(a, b)$ *and* $v(a, b)$ *be nondegenerate Lucas sequences for which* $gcd(a, b) = 1$. *Then* $|u_n| = 1$ *or 2 for* $n > 1$ *or* $|v_n| = 1$ *or 2 for* $n \geq 1$ *only in the following instances:*

(i) $n = 1,\ a = \pm 1$ *or* $\pm 2,\ v_1 = a$;

(ii) $n = 2,\ a = \pm 1$ *or* $\pm 2,\ u_2 = a$;

(iii) $n = 2,\ a$ *is odd,* $b = (\pm 1 - a^2)/2,\ v_2 = \pm 1$;

(iv) $n = 2,\ a$ *is even,* $b = (\pm 2 - a^2)/2,\ v_2 = \pm 2$;

(v) $n = 3,\ b = \pm 1 - a^2,\ u_3 = \pm 1$;

(vi) $n = 3,\ a$ *is odd,* $b = \pm 2 - a^2,\ u_3 = \pm 2$;

(vii) $n = 4,\ a = \pm 1,\ b = -2,\ v_4 = 1$;

(viii) $n = 4,\ a = \pm 2,\ b = -7,\ v_4 = 2$;

(ix) $n = 5,\ a = \pm 1,\ b = -2,\ u_5 = -1$;

(x) $n = 5,\ a = \pm 1,\ b = -3,\ u_5 = 1$;

(xi) $n = 5,\ a = \pm 12,\ b = -55,\ u_5 = 1$;

(xii) $n = 5,\ a = \pm 12,\ b = -377,\ u_5 = 1$;

(xiii) $n = 5,\ a = \pm 2,\ b = -3,\ v_5 = \pm 2$;

(xiv) $n = 7,\ a = \pm 1,\ b = -5,\ u_7 = 1$;

(xv) $n = 13,\ a = \pm 1,\ b = -2,\ u_{13} = -1$.

Proof: If $n \leq 3$, then (i) to (vi) are the only possibilities since $v_1 = u_2 = a,\ v_2 = a^2 + 2b$, and $u_3 = a^2 + b$. We note that $\rho(2)$ and $\overline{\rho}(2) \leq 3$ if the respective ranks of appearance exist. Thus, if $n \geq 4$ and $|u_n| \leq 2$, then u_n has no primitive prime divisor. Moreover, since $u_{2n} = u_n v_n$, we see that if $n \geq 2$ and $|v_n| \leq 2$, then u_{2n} has no primitive prime divisor. By Table 1 of [1], there are only finitely many possibilities for a and b such that $u_n(a,b)$ has no primitive prime divisor if $n \geq 5$ and $n \neq 6$. Checking all these terms $u_n(a,b)$ and examining $v_n(a,b)$ when $u_{2n}(a,b)$ has no primitive prime divisor, parts (vii) - (xv) are established. Since there are infinitely many sequences $u(a,b)$ for which $u_n(a,b)$ has no primitive prime divisor when $n = 4$ or 6, we need to examine the cases involving $v_3,\ u_4$, and u_6 separately.

Suppose that $v_3 = \pm 1$ or ± 2. Since $v_3 = a(a^2 + 3b)$, we must have $a = 1$ or 2 and

$$a^2 + 3b = \pm 1 \text{ or } \pm 2.$$

By straightforward calculation and use of Theorem 2.1, we obtain the contradiction that if $|a| \leq 2$, then either b is not an integer or $v(a,b)$ is degenerate. Thus, $|v_3(a,b)| \geq 3$ in all cases. It now follows that $|u_6(a,b)| \geq 3$, since $u_6 = u_3 v_3$.

Finally, suppose that

$$u_4 = u_2 v_2 = a(a^2 + 2b) = \pm 1 \text{ or } \pm 2. \tag{2.8}$$

Then $a = 1$ or $a = 2$. However, if $a = 2$, then $4 | u_4$ by (2.8). Thus, $a = 1$ and $a^2 + 2b = 2b + 1 = \pm 1$. Therefore, $b = 0$, which is impossible, or $b = -1$, which is a contradiction since $u(1,-1)$ is degenerate by Theorem 2.1. The lemma is now proved. □

3. THE MAIN THEOREMS

Theorem 3.1: *Let $u(a,b)$ be a nondegenerate Lucas sequence for which $gcd(a,b) = 1$. Suppose that $n \neq 4,\ n \neq 9$, and n is composite. Then $4 \mid \phi(|u_n|)$ except in the following instances:*

(i) $n = 6,\ a = \pm 2,\ b = -5,\ u_n = \pm 22$;
(ii) $n = 8,\ a = \pm 1,\ b = -2,\ u_n = \pm 3$;
(iii) $n = 10,\ a = \pm 1,\ b = -2,\ u_n = \pm 11$;
(iv) $n = 10,\ a = \pm 1,\ b = -3,\ u_n = \pm 31$;
(v) $n = 10,\ a = \pm 2,\ b = -3,\ u_n = \pm 22$;
(vi) $n = 15,\ a = \pm 1,\ b = -3,\ u_n = \pm 718 = \pm 2 \cdot 359$.

Proof: We suppose that n is composite, $n \neq 4, n \neq 9$, and $u_n(a,b)$ is none of the terms given in cases (i) - (vi) of Theorem 3.1. We first consider the case $n = 6$ and suppose that $4 \not| \phi(|u_6(a,b)|)$. We note that

$$u_6(a,b) = u_3 v_3 = (a^2 + b)[a(a^2 + 3b)]. \tag{3.1}$$

By Proposition 2.7 (ii)

$$gcd(a^2 + b,\ a(a^2 + 3b)) = 1 \text{ or } 2. \tag{3.2}$$

Hence, if $|a^2 + b| \geq 3$ and $|a(a^2 + 3b)| \geq 3$, then $4 \mid \phi(|u_6|)$ by (3.1), (3.2), and Proposition 2.2. However, $|v_3| = |a(a^2 + 3b)| \geq 3$ by Lemma 2.21. Thus, $|a^2 + b| = 1$ or 2.

Suppose that $a = 1$ or 2. Then, by the hypotheses, $(a,b) = (1,-2), (2,-3)$, $(1,1)$, or $(1,-3)$. However, $u_6(1,-2) = 5$, $u_6(2,-3) = -10$, $u_6(1,1) = 8$, and $u_6(1,-3) = 16$. Thus, $4 \mid \phi(|u_6(a,b)|)$ in all these cases, which is a contradiction.

Now suppose that $a \geq 3$. Since $|a^2 + b| = 1$ or 2, we have $b \leq -7$. Since

$$|(a^2 + 3b) - (a^2 + b)| = |2b| \geq 14,$$

we see that $|a^2 + 3b| \geq 12$. However,

$$gcd(a, a^2 + 3b) \mid 3,$$

since $gcd(a, b) = 1$. Noting that $3||a^2+3b$ and $|a^2+3b| > 6$ if $3|a$, we see from (3.1), Proposition 2.2, Lemma 2.3(i), and Lemma 2.4 that $4 \mid \phi(|u_6|)$, a contradiction. Our treatment of the case $n = 6$ is now complete.

Next we assume that $n = 2k$, where $k \geq 4$, u_n has a primitive prime divisor, and $|u_k| \geq 3$. We note by Theorem 2.14 and Lemma 2.21 that these conditions hold if $k \geq 8$ and $k \neq 9, 13$ or 15. Then, by Lemma 2.3(ii), $4 \mid \phi(|u_n|)$.

Suppose that $n = 8$. Then $|u_4| \geq 3$ by Lemma 2.21. Thus, $4 \not| \phi(|u_8|)$ only if u_8 has no primitive prime divisor. By Table 1 of [1], $u_8(a, b)$ has no primitive prime divisor only if $(a, b) = (1, -2)$ or $(2, -7)$. The case $a = 1$, $b = -2$ is excluded by hypothesis. Since $|u_4(2, -7)| = 20$, $4 \mid \phi(|u_8(2, -7)|)$ by Lemma 2.3.

Next, assume that $n = 10$. By Table 1 of [1], $u_{10}(a, b)$ has no primitive prime divisor only if $(a, b) = (2, -3)$, $(5, -7)$, or $(5, -18)$. The case $a = 2$, $b = -3$ is excluded by hypothesis. We note that if $a = 5$, then $u_2(a, b) = a = 5$ and $4 \mid \phi(|u_{10}(a, b)|)$. Now suppose that $4 \not| \phi(|u_{10}(a, b)|)$ and $u_{10}(a, b)$ has a primitive prime divisor. Then $|u_5(a, b)| \leq 2$ by Lemma 2.3 (ii). By Lemma 2.21, we must have $(a, b) = (1, -2)$, $(1, -3)$, $(12, -55)$, or $(12, -377)$. The cases $(a, b) = (1, -2)$ or $(1, -3)$ are excluded by hypothesis. If $a = 12$, then $u_2(a, b) = a = 12$, and $4 \mid \phi(|u_{12}(a, b)|)$ by Lemma 2.3 (i).

Now assume that $n = 12$, 18, or 30. Then, by our earlier consideration of the case $n = 6$ in this proof, we saw that $4 \mid \phi(|u_6(a, b)|)$ if $(a, b) \neq (2, -5)$, and consequently $4 \mid \phi(|u_n(a, b)|)$ in these cases if $(a, b) \neq (2, -5)$. Since $|u_4(2, -5)| = 12$, $4 \mid \phi(|u_{12}(2, -5)|)$. Moreover, $u_{2k}(2, -5)$ has a primitive prime divisor and $|u_k(2, -5)| \geq 3$ when $k = 9$ or 15. Then, by our earlier discussion, $4 \mid \phi(|u_n(2, -5)|)$ when $n = 18$ or 30.

Now suppose that $n = 2k$, where $k = 7$ or 13. By Theorem 2.14, $u_{2k}(a, b)$ has a primitive prime divisor. Thus, by Lemma 2.3 (ii), $4 \not| \phi(|u_{2k}(a, b)|)$ only if $|u_k(a, b)| \leq 2$. By Lemma 2.21, either $k = 7$ and $(a, b) = (1, -5)$ or $k = 13$ and $(a, b) = (1, -2)$. By inspection, we see that $|u_{14}(1, -5)| = 559 = 13 \cdot 43$ and $|u_{26}(1, -2)| = 181$, which is a prime congruent to 1 modulo 4. Hence, $4 \mid \phi(|u_{2k}(a, b)|)$ in these two instances.

We finally assume that n is odd and $n \neq 9$. By Theorem 2.14, $u_n(a, b)$ has a primitive prime divisor. By Lemma 2.3 (ii), $4 \not| \phi(|u_n(a, b)|)$ only if $|u_m(a, b)| \leq 2$ for every proper divisor m of n. By Lemma 2.21, $|u_m(a, b)| \leq 2$ for m odd only if $m =$1, 3, 5, 7, or 13. By inspection of parts (v) - (vi), (ix) - (xii), and (xiv) - (xv) of Lemma 2.21, we see that it is possible that $4 \not| \phi(|u_n(a, b)|)$ only in the following cases:

(a) $n = 15$, $(a, b) = (1, -2)$ or $(1, -3)$;
(b) $n = 25$, $(a, b) = (1, -2)$, $(1, -3)$, $(12, -55)$, or $(12, -377)$;
(c) $n = 39$, $(a, b) = (1, -2)$;
(d) $n = 49$, $(a, b) = (1, -5)$;
(e) $n = 65$, $(a, b) = (1, -2)$;
(f) $n = 169$, $(a, b) = (1, -2)$.

By inspection and computer calculations using Mathematica, we see that $|u_{15}(1, -2)| = 89$, $|u_{25}(1, -2)| = 4049$, $u_{25}(1, -3)| = 282001$, and $|u_{65}(1, -2)| = 335257649$ are all primes

congruent to 1 modulo 4. Moreover, $|u_{15}(1,-3)| = 718 = 2 \cdot 359$, $|u_{25}(12,-377)|$ is the product of three odd primes, and $|u_n(a,b)|$ is the product of two odd primes in all other instances in cases (a) - (f). The proof is now complete. □

Remark 3.2: *From the above proof, Lemma 2.21, and Theorem 2.14, it is interesting to note that apart from* $u_{25}(\pm 1,-3)$, *which is prime,* $u(\pm 1,-2)$ *is the only Lucas sequence* $u(a,b)$ *that has the largest composite indices n for which* $|u_n(a,b)|$ *is a prime, namely,* $n = 15,\ 25,\ 26,$ *and 65. Moreover,* $|u_4(\pm 1,-2)| = 3,\ |u_6(\pm 1,-2)| = 5,\ |u_8(\pm 1,-2)| = 3,\ |u_9(\pm 1,-2)| = 17,$ *and* $|u_{10}(\pm 1,-2)| = 11$ *are all primes. Thus,* $u(\pm 1,-2)$ *possesses all the composite indices n for which* $|u_n(a,b)|$ *may be a prime for some integers a and b.*

Corollary 3.3: *Let* $u(a,b)$ *be a nondegenerate Lucas sequence for which* $gcd(a,b) = 1$ *and* $D > 0$. *If n is composite, then* $4 \mid \phi(|u_n|)$, *except when* $n = 4,\ a = \pm 1,$ *and* $b = (p^k - 1)/2$ *for some prime* $p \equiv 3 \pmod 4$ *and* $k \geq 1$.

Proof: By Theorem 3.1, it suffices to prove that $4 \mid \phi(|u_n|)$ if $n = 9$ or $n = 4$ with the stated exceptions. We first suppose that $n = 4$ and $a \geq 2$. Note that $u_4 = a(a^2 + 2b)$. If $b \geq 1$, then

$$a^2 + 2b \geq 6. \tag{3.3}$$

Since $D > 0$, we see that if $b \leq -1$, then

$$a^2 + 2b = a^2 + 4b - 2b = D - 2b \geq -2b + 1 \geq 3. \tag{3.4}$$

If a is even, then by (3.3) and (3.4), $a^2 + 2b$ is also even and $a^2 + 2b \geq 3$. Hence, $4 | u_4$ and $u_4 > 4$, implying that $4 \mid \phi(|u_4|)$.

If $a \geq 3$ is odd, then $a^2 + 2b$ is also odd. Since $gcd(a,b) = 1$, we have $gcd(a, a^2 + 2b) = 1$. Noting that $a^2 + 2b \geq 3$, it follows by Proposition 2.2 that $\phi(|u_4|) = \phi(a(a^2 + 2b))$ is divisible by 4.

We now assume that $a = 1$. Then

$$u_4 = a(a^2 + 2b) = 2b + 1. \tag{3.5}$$

Since $a = 1$ and $D = a^2 + 4b > 0$, we must have $b > 0$. Thus, $u_4 = 2b + 1 > 0$. However, by Lemma 2.4, $4 \not| \phi(m)$ if and only if $m = 1,\ 2,\ 4,\ p^k$, or $2p^k$, where p is a prime congruent to 3 (mod 4) and $k \geq 1$. Note that $2b + 1$ cannot be 1 or even. Thus, by (3.5), $4 \mid \phi(u_4)$ unless $a = 1$ and $b = (p^k - 1)/2$ for some prime $p \equiv 3 \pmod 4$ and $k \geq 1$.

We finally suppose that $n = 9$. By Theorem 2.14, u_9 has an odd primitive prime divisor. If $|u_3| \geq 3$, it follows by Lemma 2.3(ii) that $4 \mid \phi(|u_9|)$. By Lemma 2.8, $|u_3| < 3$ only if $a = b = 1$. However, $u_9(1,1) = 34$ and $4 \mid \phi(|u_9(1,1)|)$. □

Theorem 3.4: *Let* $u(a,b)$ *be a nondegenerate Lucas sequence for which* $D > 0$ *and* $gcd(a,b) = 1$. *Then* $4 \mid \phi(|u_n|)$ *for* $n \geq 3$ *if at least one of the following conditions holds:*

(i) $-b$ *is a square.*

(ii) b *is a square,* $n \neq 3$ *if* $|a| = b = 1,$ *and* $n \neq 4$ *if* $a = \pm 1$.

(iii) $b \equiv 1$ *(mod 4),* $a \equiv 1$ *(mod 2),* $n \neq 3,$ *and* $n \neq 4$ *if* $a = \pm 1$.

(iv) $b \leq -2,\ |a| = -b + 1,\ b \equiv 0$ *or 1 (mod 4), and* $n \neq 5$ *if* $b = -3$.

Proof: We first adapt Montgomery's proof in [15] and prove (i) and (ii) in the special case that $b = \pm 1$. We note that if $b = -1$, then $a \geq 3$, since $D = a^2 + 4b > 0$. Assume that $n \geq 3$ if $a \neq 1$ and $n \geq 5$ if $a = 1$. By Proposition 2.11 (i),

$$u_{n-1}^2 - u_{n-2}u_n = (-b)^{n-2} \equiv u_{n-1}^2 \equiv \pm 1 \pmod{u_n}. \tag{3.6}$$

We claim that the four integers $\pm 1, \pm u_{n-1}$ are incongruent modulo u_n. This is easy to see if $a = b = 1$ and $n \geq 5$. In all other cases, one sees that $u_n > 2u_{n-1}$ for $n \geq 3$, and the result follows.

We now see from (3.6) that the four integers $\pm 1, \ \pm u_{n-1}$ form a subgroup of the multiplicative group G of units of the ring of integers modulo u_n. This subgroup is the Klein 4-group if $b = -1$ or both $b = 1$ and n is even, and is the cyclic group of order 4 if $b = 1$ and n is odd. Since $|G| = \phi(u_n), \ 4 \mid \phi(u_n)$ by Lagrange's Theorem.

We now prove the remainder of parts (i) and (ii) and also parts (iii) and (iv). By Corollary 3.3, $4 \mid \phi(|u_n|)$ if n is composite and it is not the case that $n = 4$ and $a = 1$. Thus, it suffices to consider only the cases in which $n = 4$ and $a = 1$ or $n \geq 3$ is a prime.

(i) Since $D > 0, \ a \geq 3$. By Theorem 2.17 (i) and Proposition 2.2, if $n \geq 5$ is odd, then u_n has two distinct odd primitive prime divisors, and hence $4 \mid \phi(|u_n|)$. Thus, $4 \mid \phi(|u_n|)$ for $n \geq 4$.

We now show that $4 \mid \phi(|u_3|)$. Let $b = -b_0^2$, where $b_0 > 0$. Then

$$u_3 = a^2 + b = a^2 - b_0^2 = (a + b_0)(a - b_0),$$

where $gcd(a, b_0) = 1$. If $a \equiv b_0 \equiv 1 \pmod 2$, then $a^2 \equiv b_0^2 \equiv 1 \pmod 8$, and $8|u_3$. Hence, $4 \mid \phi(|u_3|)$ in this case. Now assume that $a \not\equiv b_0 (\mathrm{mod}\ 2)$. Since $D = a^2 - 4b_0^2 > 0, \ a > 2b_0$. Thus, $a - b_0 \geq 3$, since $a - b_0 \equiv 1 \pmod 2$. Therefore, there exist distinct odd primes p and q such that $p|a + b_0$ and $q|a - b_0$, and $4 \mid \phi(|u_3|)$ in this case also.

(ii) Let $b = b_1^2$, where $b_1 > 0$. Then $D > 0$ and $gcd(u_n, b_1) = 1$ for $b \geq 1$ by Proposition 2.7 (i). By Proposition 2.11 (ii),

$$u_{2n-1} = (b_1 u_{n-1})^2 + u_n^2. \tag{3.7}$$

Then $gcd(b_1 u_{n-1}, u_n) = 1$ since $gcd(u_{n-1}, u_n) = 1$. Thus, if $u_{2n+1} > 2$, then u_{2n+1} has a prime factor congruent to 1 modulo 4, and hence $4 \mid \phi(u_{2n+1})$. By Lemma 2.8, $u_{2n+1} > 2$ if $2n + 1 \geq 3$ and it is not the case that both $a = b = 1$ and $2n + 1 = 3$. The result now follows.

(iii) By inspection, one sees that $u(a, b)$ has a period modulo 4 of length equal to 6 and that $u_n \equiv 1 \pmod 4$ if $n \equiv \pm 1 \pmod 6$. By Lemma 2.8, $u_n \geq 5$ if $n \geq 5$. Thus, by Lemma 2.4, $4 \not| \phi(u_n)$ for $n > 3$ an odd prime only if u_n is a square. However, by Theorem 2.19 (iii), u_n is not a square if $n > 3$ is odd.

(iv) We note that if $b \leq -2$ and $a = -b + 1$, then $D = (b + 1)^2 > 0$. Since $a > 1$, it suffices to show that $4 \mid \phi(u_n)$ if $n \geq 3$ is odd and $n \neq 5$ if $b = -3$. We observe that either $a \equiv 0, \ b \equiv 1 \pmod 4$ or $a \equiv 1, \ b \equiv 0 \pmod 4$. By inspection and Lemma 2.8, we see that $u_n > 1$ if $n \geq 3$ and $u_n \equiv 1 \pmod 4$ if $n \equiv 1 \pmod 2$. Thus, by Lemma 2.4, $4 \not| \phi(u_n)$ for $n \geq 3$ and n odd only if u_n is a square. However, by Theorem 2.19 (ii), u_n cannot be a square if n is odd, $n \geq 3$, and it is not the case that $n = 5$ and $b = -3$. □

Theorem 3.5: *Let $v(a_1, b_1)$ be a nondegenerate Lucas sequence for which $gcd(a_1, b_1) = 1$. Let $k \geq 2$ and let $a = \pm v_k(a_1, b_1)$ and $b = (-1)^{k+1} b_1^k$. Then $u(a, b)$ is a nondegenerate Lucas sequence for which $u_n(a, b)$ and both $D = D(a, b)$ and $D_1 = D(a_1, b_1)$ have the same sign. Let p denote an arbitrary prime.*

(i) Suppose $D > 0$. Then $4 \mid \phi(|u_n(a,b)|)$ if $n \geq 3$ and it is not the case that both $k = p^t$ and $n = p$, where $t \geq 1$.

(ii) Suppose $D < 0$ and k has at least two distinct prime divisors. Then $4 \mid \phi(|u_n(a,b)|)$ for $n \geq 6$.

(iii) Suppose $D < 0$ and $k = p^i$, where $i \geq 2$. Then $4 \mid \phi(|u_n(a,b)|)$ for $n \geq 6$ and $n \neq p$.

(iv) Suppose $D < 0$ and $k = p$. Then $4 \mid \phi(|u_n(a,b)|)$ if $n \geq 6$, $n \neq p$, and it is not the case that either $n = 7$, $a_1 = \pm 1$, $b_1 = -5$, or $n = 13$, $a_1 = \pm 1$, $b_1 = -2$.

Proof: We first note that by Lemma 2.20, $u(a,b)$ is a nondegenerate Lucas sequence, $gcd(a,b) = 1$, both D and D_1 have the same sign, and

$$u_n(a,b) = \frac{u_{kn}(a_1,b_1)}{u_k(a_1,b_1)}. \tag{3.8}$$

We prove parts (i) - (iv) together. We assume throughout the proof that $a > 0$. First assume that $D > 0$. Since $a = v_k(a_1,b_1)$ and $D_1 > 0$, it follows from Lemma 2.8 that $a \geq 3$. We now see from Corollary 3.3 that $4 \not\mid \phi(|u_n(a,b)|)$ for $n \geq 3$ only if n is a prime. Now assume that $|b_1|$ is a square. Then $|b| = |(-1)^{k+1}b_1^k|$ is also a square. It now follows from parts (i) and (ii) of Theorem 3.4 that $4 \mid \phi(|u_n(a,b)|)$ for $n \geq 3$. Thus, if $D > 0$, we need only treat the cases in which $|b_1|$ is not a square and $n \geq 3$ is a prime.

We note by Theorem 3.1 that if $4 \not\mid \phi(|u_n(a,b)|)$ where $gcd(a,b) = 1$, $n \geq 6$ is composite, and $n \neq 9$, then b is not of the form $(-1)^{k+1}b_1^k$, where $b_1 \neq 0$ and $k \geq 2$. It follows that if $D < 0$, n is composite, $n \geq 6$, and $4 \not\mid \phi(|u_n|)$, then $n = 9$. Now suppose that $D < 0$ and $n = 9$. By Table 1 of [1] and inspection, at least two of the terms $u_{9k}(a_1,b_1)$, $u_{3k}(a_1,b_1)$, and $u_9(a_1,b_1)$ have odd primitive prime divisors. Since $u_{9k}(a_1,b_1)$ and $u_{3k}(a_1,b_1)$ have odd primitive prime divisors if $9|k$ by Theorem 2.14, it follows from (3.8) that $4 \mid \phi(|u_9(a,b)|)$. Therefore, if $D < 0$, we only need to consider the cases in which $n \geq 6$ is a prime.

From here on until the end of the proof, we assume that n is a prime greater than or equal to 3 if $D > 0$ and n is a prime greater than 6 if $D < 0$. Suppose that k has a prime factor p different from n. First suppose that $D > 0, n = 3, k = 2$ or 4, and $u_6(a_1,b_1)$ has no primitive prime divisor. By Table 3 of [1] and Lemma 2.10 (iii), if $(a_1,b_1) \neq (3,-2)$, then $a_1 \equiv b_1 \equiv 1 \pmod 2$, which implies that $8|u_6(a_1,b_1)$ and $8|u_{12}(a_1,b_1)$, while $2 \not| u_2(a_1,b_1)u_4(a_1,b_1)$. Hence, $4 \mid \phi(u_3(a,b))$ in these cases. If $(a_1,b_1) = (3,-2)$, then $u_6(a_1,b_1)$ has no primitive prime divisor,

$$u_6(a_1,b_1)/u_2(a_1,b_1) = 63/3 = 3 \cdot 7$$

and

$$u_{12}(a_1,b_1)/u_4(a_1,b_1) = 4095/15 = 3 \cdot 7 \cdot 13.$$

Thus, $4 \mid \phi(u_3(a,b))$ in these cases also.

Now assume that it is not the case that $D > 0, n = 3$, $k = 2$ or 4, and $u_6(a_1,b_1)$ has no primitive prime divisor. Then, by Theorems 2.13 and 2.14, both $u_{kn}(a_1,b_1)$ and $u_{kn/p}(a_1,b_1)$ have odd primitive prime divisors. Since neither kn nor kn/p divides k, it follows that $4 \mid \phi(|u_n(a,b)|)$.

Finally, assume that $k = p^j$, where $j \geq 1$, $n \neq p$, and it is not the case that either $n = 7$, $j = 1$, $a_1 = 1$, $b_1 = -5$ or $n = 13$, $j = 1$, $a_1 = 1$, $b_1 = -2$. Then, by Table 1 of [1], both $u_{kn}(a_1,b_1)$ and $u_n(a_1,b_1)$ have odd primitive prime divisors. Thus, by (3.8), $4 \mid \phi(|u_n(a,b)|)$. The result now follows. □

Remark 3.6: *We keep the notation of Theorem 3.5. Let $p \neq 5$ be an arbitrary prime. Using similar arguments as those in the proof of Theorem 3.5, it can be shown that if $D < 0$, then $4 \mid \phi(|u_5(a,b)|)$ if it not the case that*

(i) $k = 2$ and $(a_1, b_1) = (\pm 2, -3)$,

or

(ii) $k = p$ and $(a_1, b_1) = (\pm 1, -2)$, or $(\pm 1, -3)$, or $(\pm 12, -55)$, or $(\pm 12, -377)$,

or

(iii) $k = 5^i$, where $i \geq 1$.

Theorem 3.7: *Let $u(a,b)$ be a Lucas sequence for which $a \neq 0$ and $d = gcd(a,b) > 1$. Suppose further that $D = 0$ or $b = 0$ or $u(a,b)$ is nondegenerate. Suppose that $d \neq p^k$, where $p \equiv 3 \pmod 4$ is a prime and $k \geq 1$. Then $4 \mid \phi(|u_n|)$ for $n \geq 6$. Moreover, the following also hold:*

(i) If $d \neq 2$, $d \neq 4$, and $d \neq 2p^k$, where $p \equiv 3 \pmod 4$ is a prime and $k \geq 1$, then $4 \mid \phi(|u_n|)$ for $n \geq 2$.

(ii) If $d = 4$ or $d = 2p^k$, where $p \equiv 3 \pmod 4$ is a prime and $k \geq 1$, then $4 \mid \phi(|u_n|)$ for $n \geq 4$.

(iii) If $d = 2$ and it is not the case that $n = 5$ and $(a,b) = (\pm 2, -10)$, $(\pm 4, -6)$, or $(\pm 4, -42)$, then $4 \mid \phi(|u_n|)$ for $n \geq 4$.

(iv) If $(a,b) = (\pm 4, -6)$ or $(\pm 4, -42)$, then $4 \mid \phi(|u_n|)$ for $n \geq 3$ and $n \neq 5$.

(v) If $(a,b) = \pm(2, -10)$, then $4 \mid \phi(|u_n|)$ for $n \geq 4$ and $n \neq 5$.

Proof: It suffices to prove parts (i) - (iii). Parts (iv) and (v) then follow by inspection. We note that if $b = 0$ and $a \neq 0$, then $u_n = a^{n-1} \neq 0$ for $n \geq 1$. If $D = 0$ and $a \neq 0$, then by (2.4), $u_n = n(a/2)^{n-1} \neq 0$ for $n \geq 1$. It now follows from the discussion before Theorem 2.1 that $u_n \neq 0$ for $n \geq 1$ whenever the hypotheses are satisfied.

(i) By Lemma 2.12, $d | u_n$ for $n \geq 2$, implying by Proposition 2.2(iii) and Lemma 2.4 that $4 \mid \phi(|u_n|)$ for $n \geq 2$.

(ii) By Lemma 2.12, $d^2 | u_n > 4$. The result now follows.

(iii) By Lemma 2.12, $4 | u_n$ for $n \geq 4$ and $8 | u_n$ for $n \geq 6$. Thus, $4 \mid \phi(|u_n|)$ for $n \geq 6$. We further note that $u_4 = a(a^2 + 2b)$. Since $2|a$ and $2|b$, it follows that $4|a^2 + 2b$, and hence, $8|u_4$. Thus, $4 \mid \phi(|u_4|)$ also. Moreover, $\phi(|u_5|)$ will be divisible by 4 if it can be shown that $|u_5| > 4$.

Suppose that $|u_5| = 4$. Let $a = 2c$ and $b = 2g$ where c is a positive integer and either c or g is odd. Then, by Proposition 2.11(ii),

$$u_5 = bu_2^2 + u_3^2 = a^2 b + (a^2 + b)^2 = 4(g^2 + 6c^2 g + 4c^4) = \pm 4. \tag{3.9}$$

Therefore,

$$g^2 + 6c^2 g + 4c^4 \pm 1 = 0,$$

which implies that

$$g = \frac{-6c^2 \pm \sqrt{20c^4 \pm 4}}{2}. \tag{3.10}$$

Hence, $20c^4 \pm 4 = \rho^2$ for some non-negative integer ρ. Thus,

$$\rho^2 - 5(2c^2)^2 = \pm 4. \tag{3.11}$$

It is well known that (ρ, c) is a solution to (3.11) if and only if $\rho = L_n$ and $2c^2 = F_n$ for some positive integer n. By Theorem 2.19(i), F_n is twice a positive square if and only if $n = 3,\ F_n = 2$, and $c = 1$, or $n = 6,\ F_n = 8$, and $c = 2$. Thus the only possibilities for a are $a = 2(1) = 2$ or $a = 2(2) = 4$. Noting that $b = 2g$, it follows from (3.10) that if $a = 2$ and $c = 1$, then $b = -2$ or $b = -10$, while if $a = 4$ and $c = 2$, then $b = -6$ or $b = -42$. We note that we cannot have $a = 2,\ b = -2$, since then $D \neq 0$ and $u(a, b)$ is degenerate by Theorem 2.1. We observe that $u_5 = -4$ if $a = 2,\ b = -10$, while $u_5 = 4$ if either $a = 4,\ b = -6$ or $a = 4,\ b = -42$. The result now follows. □

Theorem 3.8: *Let $u(a, b)$ be a nondegenerate Lucas sequence. Then there exists an effectively computable constant $C(a, b)$, dependent on a and b, such that $4 \mid \phi(|u_n|)$ for $n > C(a, b)$ if at least one of the following conditions holds:*

(i) $gcd(a, b) > 1$,

(ii) $-b$ *is a square,*

(iii) $b \equiv 0$ *or* $1 \pmod 4$ *and* $D > 0$.

Proof:

(i) Let p be a prime dividing $gcd(a, b)$. By Lemma 2.12, $p^2 | u_n(a, b)$ for $n \geq 4$. By Theorem 2.16, there exists a constant $C_1(a, b) \geq 4$ such that if $n > C_1(a, b)$, then $u_n(a, b)$ has an odd primitive prime divisor q. Then $p^2 q | u_n(a, b)$. Hence, by Proposition 2.2, $4 \mid \phi(|u_n(a, b)|)$ for all $n > C_1(a, b)$.

(ii) By Theorem 3.4 (i) and part (i) of this theorem, we can assume that $gcd(a, b) = 1$ and $D < 0$. By Theorem 2.17 (ii), there exists a constant $C_2(a, b)$ such that if $n > C_2(a, b)$, then $u_n(a, b)$ has at least two odd primitive prime divisors. Hence, $4 \mid \phi(|u_n(a, b)|)$ if $n > C_2(a, b)$ and n is odd. The result now follows by Theorem 3.1.

(iii) Since $D > 0$, we have $u_n > 0$ for $n \geq 1$ by Remark 2.9. By part (i), we can assume that $gcd(a, b) = 1$. By Theorem 3.1, it suffices to show that $4 \mid \phi(u_n(a, b))$ for $n > 3$ a prime. One sees by inspection that $u(a, b)$ has a period modulo 4 less than or equal to 6 and that if $n \equiv 1$ or $5 \pmod 6$, then $u_n(a, b) \equiv 1 \pmod 4$. It now follows that if $n > 3$ is a prime, then $u_n \equiv 1 \pmod 4$. By Lemma 2.4, if $u_n \equiv 1 \pmod 4$ and $4 \not| \phi(u_n)$, then u_n is a square. However, by Theorem 2.19 (iv), there exists a constant $C_3(a, b) > 3$ such that if $n > C_3(a, b)$, then $u_n(a, b)$ is not a square. The result now follows. □

Theorem 3.9: *Let $u(a, b)$ be a Lucas sequence for which $a \neq 0$. Let S be the set of those positive integers n for which $4 \mid \phi(|u_n|)$. Then the natural density of S in the set of positive integers is equal to 1 in the following cases:*

(i) $u(a, b)$ *is nondegenerate.*

(ii) $D = 0$.

(iii) $b = 0$ *and* $a \neq p^k$, *where* $p \equiv 3 \pmod 4$ *is a prime and* $k \geq 0$.

Proof:

(i) If $gcd(a, b) > 1$, then S has density 1 by Theorem 3.8. If $gcd(a, b) = 1$, then, by Theorem 3.1, $4 \mid \phi(|u_n|)$ for $n > 15$ unless n is a prime. Since the set of primes has density 0 in the set of positive integers, the result follows.

(ii) We observe that

$$u_n = n(a/2)^{n-1} \tag{3.12}$$

by the Binet formula (2.4). Noting that a is even and $(a/2) | gcd(a, b)$ if $D = 0$, it follows from Lemma 2.4 that $4 \mid \phi(|u_n|)$ for $n \geq 3$ if $a/2 \neq p^k$, where $p \equiv 3 \pmod 4$ is a prime and $k \geq 0$. If $a/2 = p^i$, where $p \equiv 3 \pmod 4$ is a prime and $i \geq 1$, then by (3.12) and

Lemma 2.4, $4 \not| \phi(|u_n|)$ if and only if $n = p^j$ or $n = 2p^j$ for some nonnegative integer j. If $a/2 = 1$, we see by (3.12) and Lemma 2.4 that $4 \not| \phi(|u_n|)$ if and only if $n = 1,\ 2,\ 4,\ q^k$, or $2q^k$, where q is any prime congruent to 3 modulo 4 and $k \geq 1$. Since the density of the set of primes and prime powers in the set of positive integers is equal to 0, the result follows.

(iii) The result follows from Theorem 3.7. □

Remark 3.10: *More can be said here about the order of the prime* 2 *in the factorization of* $\phi(|u_n|)$. *Indeed, assume that* $u(a,b)$ *is nondegenerate. For a positive integer* n *we write* $\omega(n)$ *for the number of distinct prime factors of* n. *By a classical result of Túran and Kubilius,* $\omega(n) = (1+o(1)) \log\log n$ *holds for almost all positive integers* n. *That is, if* $\varepsilon > 0$ *is arbitrarily small, then the set of positive integers* n *such that* $|\omega(n) - \log\log n| < \varepsilon \log\log n$ *is of asymptotic density* 1. *Let* $\tau(n)$ *be the number of divisors of* n. *Clearly,* $\tau(n) \geq 2^{\omega(n)} = (\log n)^{(1+o(1))\log 2}$. *By the Primitive Divisor Theorem 2.14,* u_n *has at least* $\tau(n) - 13$ *distinct prime factors (i.e., if* $d|n$ *is any divisor of* n *not in the set* $\{1,2,3,4,5,6,7,8,10,12,13,18,30\}$, *then there exists a primitive prime factor of* $u_d|u_n$). *Of those primes, at most one is even, and for each one of the remaining odd prime factors* p *of* u_n *we get a factor* 2 *in* $\phi(|u_n|)$ *via the fact that* $2|(p-1)|\phi(|u_n|)$. *It now follows easily that the order of* 2 *in the factorization of* $\phi(|u_n|)$ *is at least* $\tau(n) - 14 = (\log n)^{(1+o(1))\log 2}$ *for most positive integers* n.

Theorem 3.11: *Let the fixed positive integer* b *be a square.*

(i) If $a \neq 0$, $gcd(a,b) = 1$, *and* a *has a prime factor* $p \equiv 1 \pmod 4$, *then* $u_n(a,b)$ *has a prime divisor of the form* $4r+1$ *for* $n \geq 2$.

(ii) There exist infinitely many nonzero integers a *such that* $gcd(a,b) = 1$, a *does not have a prime factor* $p \equiv 1 \pmod 4$, *and* $u_n(a,b)$ *has a prime divisor of the form* $4r+1$ *for* $n \geq 3$.

Proof:

(i) By the proof of Theorem 3.4 (ii), u_{2k+1} has a prime factor $q \equiv 1 \pmod 4$ for $k \geq 1$. Let $p \equiv 1 \pmod 4$ be a prime factor of $u_2 = a$. Then $p|u_{2k}$ for $k \geq 1$ since $u_2|u_{2k}$. The assertion now follows.

(ii) Let $b = b_1^2$, where $b_1 > 0$. Assume that a is any positive integer such that it is not the case that $a = b = 1$. Again, by the proof of Theorem 3.4 (ii), u_{2k+1} has a prime factor $q \equiv 1 \pmod 4$, where $k \geq 1$. Therefore, if n has an odd divisor $m \geq 3$, then u_n has a prime factor of the form $4r+1$, since $u_m|u_n$. It thus suffices to show that there exist infinitely many positive integers a such that $u_2 = a$ does not have a prime factor $p \equiv 1 \pmod 4$, but u_4 does have a prime factor of the form $4r+1$. Since $u_4|u_{2^m}$ for $m \geq 2$, it would then follow that u_{2^m} has a prime factor of the form $4r+1$ for $m \geq 2$. Let s be any prime of the form $8t+1$ such that $s \not| b$. By Dirichlet's theorem on the infinitude of primes in arithmetic progressions, there exist infinitely many such primes s. Since $(-2/s) = 1$ by the law of quadratic reciprocity, where $(-2/s)$ denotes the Legendre symbol, there exists an integer c such that $0 < c < s$ and $c^2 \equiv -2 \pmod s$. By Dirichlet's theorem and the Chinese remainder theorem, there exist infinitely many primes a such that $a > b$, $a \equiv cb_1 \pmod s$, and $a \equiv 3 \pmod 4$. Then $gcd(a,b) = 1$, a has no prime factor $p \equiv 1 \pmod 4$, and

$$u_4(a,b) = a(a^2 + 2b_1^2) \equiv a(c^2 b_1^2 + 2b_1^2) \equiv a(-2b_1^2 + 2b_1^2) \equiv 0 \pmod s.$$

The result now follows since $s \equiv 1 \pmod 4$. □

Theorem 3.12: *Let* $u(a,b)$ *be a nondegenerate Lucas sequence such that* b *is a square,* $gcd(a,b) = 1$, *and it is not the case that* $|a| = b = 1$. *Suppose there exists an integer* $k \geq 0$

such that $v_{2^k}(a,b)$ has a prime factor of the form $4r+1$ and that k is the least such integer. Then u_n has a prime divisor of the form $4r+1$ for $n \neq 2^i$, where $0 \leq i \leq k$.

Proof: As in the proof of Theorem 3.4 (ii), if n has an odd divisor $j \geq 3$, then u_n has a prime factor of the form $4r+1$. By repeatedly applying the formula $u_{2n} = u_n v_n$ and noting that $u_1 = 1$, we see that

$$u_{2^m} = v_1 v_2 v_4 \cdots v_{2^{m-1}}. \tag{3.13}$$

Therefore, by (3.13), if $m \geq k+1$, then u_{2^m} has the divisor v_{2^k} and thus a prime factor of the form $4r+1$. The result now follows. □

Remark 3.13: *We conjecture that for any nondegenerate Lucas sequence $v(a,b)$ for which b is a square and $gcd(a,b) = 1$, there exists an integer k such that v_{2^k} has a prime factor $p \equiv 1 \pmod 4$. It would then follow from Theorems 1.1 and 3.11 that there exists an integer $C(a,b)$, dependent on a and b, such that $u_n(a,b)$ has a prime factor of the form $4r+1$ for $n > C(a,b)$. We note that if $|a| = b = 1$, then 5 is the smallest value of k such that v_{2^k} has a prime factor of the form $4r+1$ and that the prime 4481 divides $v_{32}(\pm 1, 1)$.*

ACKNOWLEDGMENT

We thank the anonymous referees for suggestions that greatly improved the quality of this paper. The first author's research was partly supported by grant PAPIIT IN104505.

REFERENCES

[1] Yu. Bilu, G. Hanrot, & P. M. Voutier. "Existence of Primitive Divisors of Lucas and Lehmer Numbers." *J. Reine Angew. Math.* **539** (2001): 75-122.
[2] John L. Brown, Jr. "Incomplete Solution to H-54." *The Fibonacci Quarterly* **4** (1966): 334-335.
[3] D. M. Burton. *Elementary Number Theory*, Fifth Edition. McGraw-Hill, New York, 2002.
[4] R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Ann. Math.* **15** (1913): 30-70.
[5] J. H. E. Cohn. "Square Fibonacci Numbers, etc." *The Fibonacci Quarterly* **2** (1964): 109-113.
[6] J. H. E. Cohn. "Lucas and Fibonacci Numbers and Some Diophantine Equations." *Proc. Glasgow Math. Assoc.* **7** (1965): 24-28.
[7] P. Hilton, J. Pedersen and L. Somer. "On Lucasian Numbers." *The Fibonacci Quarterly* **35** (1997): 43-47.
[8] V. E. Hoggatt, Jr. and H. Edgar. "Another Proof that $\Phi(F_n) \equiv 0$ Mod 4 for all $n > 4$." *The Fibonacci Quarterly* **18** (1980): 80-82.
[9] C. Kimberling. "Problem E 2581." *Amer. Math. Monthly* **83** (1976): 197.
[10] D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. Math.* **31.2** (1930): 419-448.
[11] L. G. Lekkerkerker. "Prime Factors of the Elements of Certain Sequences of Integers." *Proc. Amsterdam Akad.* (Series A) **56** (1953): 265-280.
[12] D. Lind. "Problem H-54." *The Fibonacci Quarterly* **3** (1965): 4.
[13] W. Ljunggren. "New Propositions About the Indeterminate Equation $(x^n - 1)/(x - 1) = y^q$." *Norske Mat. Tidsskrift* **25** (1943): 17-20.

[14] W. L. McDaniel. "On Fibonacci and Pell Numbers of the Form kx^2 (Almost Every Term Has a $4r+1$ Prime Factor)." *The Fibonacci Quarterly* **40** (2002): 41-42.
[15] P. Montgomery. "Solution to Problem E 2581." *Amer. Math. Monthly* **84** (1977): 488.
[16] A. Pethő. "Perfect Powers in Second Order Linear Recurrences." *J. Number Theory* **15** (1982): 5-13.
[17] P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, New York, 1996.
[18] P. Ribenboim and W. L. McDaniel. "The Square Terms in Lucas Sequences." *J. Number Theory* **58** (1996): 104-123.
[19] A. Rotkiewicz. "On Lucas Numbers with Two Intrinsic Divisors." *Bull. Acad. Polon. Sér. Math. Astr. Phys.* **10** (1962): 229-232.
[20] A. Schinzel. "The Intrinsic Divisors of Lehmer Numbers in the Case of Negative Discriminant." *Ark. Mat.* **4** (1962): 413-416.
[21] A. Schinzel. "On Primitive Prime Factors of Lehmer Numbers I." *Acta Arith.* **8** (1963): 213-223.
[22] T. N. Shorey and C. L. Stewart. "On the Diophantine Equation $ax^{2t} + bx^t y + cy^2 = d$ and Pure Powers in Recurrence Sequences." *Math. Scand.* **52** (1983): 24-36.
[23] T. N. Shorey and R. Tijdeman. *Exponential Diophantine Equations.* Cambridge Univ. Press., Cambridge, 1986.
[24] M. Ward. "Prime Divisors of Second Order Recurring Sequences." *Duke. Math. J.* **21** (1954): 607-614.

AMS Classification Numbers: 11B39, 11A25, 11B37

✠ ✠ ✠