GENERALIZATION OF A THEOREM OF BRUCKMAN ON DICKSON PSEUDOPRIMES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

ABSTRACT. Let the Lucas numbers $\{L_n\}$ be defined by $L_{n+2} = L_{n+1} + L_n$ with initial terms $L_0 = 2$, $L_1 = 1$. It is well known that if N is an odd prime, then $L_N \equiv L_1 \equiv 1 \pmod{N}$. If N is a positive odd composite integer for which the above-mentioned congruence also holds, then N is called a Dickson pseudoprime with respect to the Lucas numbers. Paul Bruckman proved that if N is a Dickson pseudoprime with respect to the Lucas numbers for which $\gcd(N, 6) = 1$, then L_N is also a Dickson pseudoprime with respect to the Lucas numbers. We generalize this theorem by Bruckman from the Lucas numbers $\{L_n\}_{n=0}^{\infty}$ to more general second-order linear recurrences.

1. INTRODUCTION

Let the Lucas numbers $\{L_n\}$ be defined by $L_{n+2} = L_{n+2} + L_n$ with initial terms $L_0 = 2$, $L_1 = 1$. It is well known that if N is an odd prime, then N satisfies the following condition:

$$L_N \equiv L_1 \equiv 1 \pmod{N} \tag{1.1}$$

(see [1, p. 1392]). It also occurs rarely that the congruence (1.1) holds if N is a positive odd composite integer. Such numbers are called *Dickson pseudoprimes with respect to the Lucas numbers* (see [7]). The first few Dickson pseudoprimes with respect to the Lucas numbers are 705, 2465, 2737, 3745, 4181, 5777, 6721 (see Table 3 of [7]). Paul Bruckman [2] proved the following theorem:

Theorem 1.1. (Bruckman) *Let N be a Dickson pseudoprime with respect to the Lucas numbers such that $\gcd(N, 6) = 1$. Then, L_N is also a Dickson pseudoprime with respect to the Lucas numbers such that $\gcd(L_N, 6) = 1$.*

We will generalize Theorem 1.1 to Dickson pseudoprimes with respect to particular second-order linear recurrences. Let $V(P, Q)$ and $U(P, Q)$ be the Lucas sequences satisfying the second-order recursion relation

$$W_{n+2} = PW_{n+1} - QW_n \tag{1.2}$$

with discriminant $D = P^2 - 4Q$, where P and Q are integers, and the initial terms are $V_0 = 2$, $V_1 = P$, $U_0 = 0$, $U_1 = 1$, respectively. We note that $\{L_n\}_{n=0}^{\infty} = V(1, -1)$. Associated with $U(P, Q)$ and $V(P, Q)$ is the characteristic polynomial

$$f(x) = x^2 - Px + Q \tag{1.3}$$

with characteristic roots α and β. We observe that $D = (\alpha - \beta)^2$. By the Binet formulas,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n. \tag{1.4}$$

Proposition 1.2 below follows from the Binet formulas (1.4).

Proposition 1.2. *Consider the Lucas sequences $U(P, Q)$ and $V(P, Q)$ with discriminant D.*

(i) *If n is a nonnegative integer, then $U_{2n} = U_n V_n$.*
(ii) *If $m \mid n$, then $U_m \mid U_n$.*
(iii) *If $m \mid n$ and n/m is odd, then $V_m \mid V_n$.*
(iv) *If $0 \le m \le n$, then $V_{m+n} - Q^m V_{n-m} = DU_m U_n$.*
(v) *If $0 \le m \le n$, then $V_{m+n} + Q^m V_{n-m} = V_m V_n$.*

The Lucas sequences $U(P,Q)$ and $V(P,Q)$ with characteristic roots α and β are called degenerate if $PQ = 0$ or α/β is a root of unity. It follows from the Binet formulas (1.4) that $U_n(P,Q)$ or $V_n(P,Q)$ can be equal to 0 for some $n > 0$ only if $U(P,Q)$ and $V(P,Q)$ are degenerate. Because the characteristic polynomial of $U(P,Q)$ and $V(P,Q)$ is a quadratic polynomial with integer coefficients, one sees that α/β can be a primitive nth root of unity only if $n \in \{1,2,3,4,6\}$. The following theorem of Ward [8, p. 613] determines all degenerate Lucas sequences $U(P,Q)$ and $V(P,Q)$.

Theorem 1.3. *Let M denote an arbitrary nonzero integer. Then, the Lucas sequences $U(P,Q)$ and $V(P,Q)$ with characteristic roots α and β are degenerate only in the following cases:*

(i) *If $Q = 0$ and P is any integer, then $D = P^2$, $U_n = P^{n-1}$, and $V_n = P^n$ for $n \ge 1$.*
(ii) *If $\alpha/\beta = 1$, then $P = 2M$, $Q = M^2$, and $D = 0$.*
(iii) *If $\alpha/\beta = -1$, then $P = 0$, $Q = M$, and $D = -4M$.*
(iv) *If α/β is a primitive cube root of unity, then $P = M$, $Q = M^2$, and $D = -3M^2$.*
(v) *If α/β is a primitive fourth root of unity, then $P = 2M$, $Q = 2M^2$, and $D = -4M^2$.*
(vi) *If α/β is a primitive sixth root of unity, then $P = 3M$, $Q = 3M^2$, and $D = -3M^2$.*

Remark 1.4. From here on, we will frequently consider the Lucas sequences $V(P,Q)$ and $U(P,Q)$ for which $Q = \pm 1$. We note that by Theorem 1.3, $V(P,\pm 1)$ and $U(P,\pm 1)$ are nondegenerate if and only if $P \neq 0$ and it is not the case that the ordered pair $(P,Q) = (\pm 1, 1)$ or $(\pm 2, 1)$. It then follows that $D > 0$ if $V(P,Q)$ and $U(P,Q)$ are nondegenerate, where $Q = \pm 1$.

It is known that if N is an odd prime such that $\gcd(N, PQ) = 1$, then the following congruence is satisfied for the given nondegenerate Lucas sequence $V(P,Q)$,

$$V_N \equiv V_1 \equiv P \pmod{N}, \tag{1.5}$$

(see [1, p. 1392]). The positive odd composite integer N is called a *Dickson pseudoprime with respect to the Lucas sequence $V(P,Q)$* if N also satisfies (1.5) (see [7]). We simply say that N is a *Dickson pseudoprime* if the Lucas sequence $V(P,Q)$ is understood. Our main result of this paper will be Theorem 1.5, which generalizes Theorem 1.1. We will prove Theorem 1.5 in Section 3.

Theorem 1.5. *Consider the nondegenerate Lucas sequences $V(P,Q)$ and $U(P,Q)$, where $P \neq 0$ and $Q = \pm 1$. Then, $D > 0$. Let N be a Dickson pseudoprime such that $\gcd(P,N) = 1$. Suppose that $3 \nmid N$ if P is odd. Then, $P \mid V_N$ and V_N/P is also a Dickson pseudoprime with respect to $V(P,Q)$. Moreover, $\gcd(V_N/P, P) = 1$ and $3 \nmid (V_N/P)$ if P is odd.*

Remark 1.6. By Theorem 1 of [6], there exist infinitely many Dickson pseudoprimes N with respect to the nondegenerate Lucas sequence $V(P,\pm 1)$, which are pairwise relatively prime. Given a Dickson pseudoprime N_1 with respect to $V(P,\pm 1)$ such that $\gcd(P,N_1) = 1$ and $3 \nmid N_1$ if P is odd, we can use Theorem 1.5 to explicitly find infinitely many other Dickson pseudoprimes N_i with respect to $V(P,\pm 1)$. Let $N_{i+1} = \frac{1}{P} V_{N_i}$ for $i \ge 1$. Then,

$$N_2, N_3, N_4, \ldots,$$

are also Dickson pseudoprimes with respect to $V(P,\pm 1)$.

2. Preliminaries

The following results will be needed to prove our main result, Theorem 1.5.

Lemma 2.1. *Let $U(P,Q)$ and $V(P,Q)$ be Lucas sequences for which $2 \nmid \gcd(P,Q)$.*

(i) *Suppose P is odd and Q is even. Then $2 \nmid U_n$ and $2 \nmid V_n$ for $n \geq 1$.*
(ii) *Suppose P is even and Q is odd. Then, $2 \mid U_n$ if and only if $2 \mid n$, and $2 \mid V_n$ for all $n \geq 0$.*
(iii) *Suppose P and Q are both odd. Then, $2 \mid U_n$ if and only if $3 \mid n$, and $2 \mid V_n$ if and only if $3 \mid n$.*

This is proved in Lemma 2.10 of [5].

Lemma 2.2. *Let $V(P,Q)$ be a Lucas sequence, where $Q = \pm 1$. Let $\lambda(3)$ denote the period of $V(P,Q)$ modulo 3.*

(i) *The Lucas sequence $V(P,Q)$ is purely periodic modulo 3.*
(ii) *If $3 \mid P$ and $Q = -1$, then $\lambda(3) = 2$ and $3 \mid V_n$ if and only if $n \equiv 1 \pmod 2$.*
(iii) *If $3 \mid P$ and $Q = 1$, then $\lambda(3) = 4$ and $3 \mid V_n$ if and only if $n \equiv 1 \pmod 2$.*
(iv) *If $P \equiv -1 \pmod 3$ and $Q = 1$, then $\lambda(3) = 1$ and $3 \nmid V_n$ for $n \geq 0$.*
(v) *If $P \equiv 1 \pmod 3$ and $Q = 1$, then $\lambda(3) = 2$ and $3 \nmid V_n$ for $n \geq 0$.*
(vi) *If $P \equiv \pm 1 \pmod 3$ and $Q = -1$, then $\lambda(3) = 8$ and $3 \mid V_n$ if and only if $n \equiv 2 \pmod 4$.*

Proof. This follows by inspection of $V(P,Q)$ modulo 3. □

The following lemma is mainly due to Hilton, Pedersen, and Somer and follows from Lemma 3 of [4] and Lemma 2.8 of [5].

Lemma 2.3. *Let $U(P,Q)$ and $V(P,Q)$ be nondegenerate Lucas sequences such that $D > 0$. Then, $|U_n|$ is increasing for $n \geq 2$ and $|V_n|$ is increasing for $n \geq 1$. Further, if $P > 0$, then $U_n > 0$ for $n \geq 1$ and $V_n > 0$ for $n \geq 0$.*

Lemma 2.4. *Consider the nondegenerate Lucas sequence $V(P,Q)$, where P is even and Q odd. Suppose that $2^k \parallel P$, where $k \geq 1$ and $2^k \parallel P$ means that $2^k \mid P$, but $2^{k+1} \nmid P$. Then, $2^k \parallel V_{2n+1}$ for $n \geq 0$.*

Proof. We proceed by induction. We observe that $2 \parallel V_0$ and $2^k \parallel V_1$. Suppose that $2 \parallel V_{2n}$ and $2^k \parallel V_{2n+1}$ for some $n \geq 0$. Then,

$$V_{2n+2} = PV_{2n+1} - QV_{2n} \equiv 0 - 2 \equiv 2 \pmod 4$$

and

$$V_{2n+3} = PV_{2n+2} - QV_{2n+1} \equiv 0 - 2^k \equiv 2^k \pmod{2^{k+1}}.$$

The result now follows. □

Lemma 2.5. *Consider the nondegenerate Lucas sequence $V(P,1)$. Then, $P \mid V_{2n+1}$ for $n \geq 0$. Moreover, $V_{2n+1}/P \equiv 1 \pmod 4$ if $n \geq 0$ and it is the case that $3 \nmid 2n+1$ when P is odd.*

Proof. We note that $V_1 = P$. It now follows from Proposition 1.2 (iii) that $P \mid V_{2n+1}$ for $n \geq 0$. Suppose that $n \geq 0$ and $3 \nmid 2n+1$ if P is odd. We now show that $V_{2n+1}/P \equiv 1 \pmod 4$.

First suppose that $P \equiv 1 \pmod 2$. Then, $\{V_n\}$ is purely periodic modulo 8 with a period equal to 3 or 6. The first eight terms of (V_n) modulo 8 starting with $n = 0$ are

$$2,\ P,\ -1,\ -2P,\ -1,\ P,\ 2,\ P.$$

It follows that $V_n/P \equiv 1 \pmod 8$ if $n \equiv \pm 1 \pmod 6$.

We now suppose that $2^k \parallel P$, where $k \geq 1$. Let $\varepsilon \in \{-1, 1\}$. Then, $\{V_n\}$ is purely periodic modulo 2^{k+2} with a period equal to 1, 2, or 4. If $k = 1$, then the first six terms of (V_n) modulo 8 starting with $n = 0$ are

$$2,\ P,\ 2,\ P,\ 2,\ P.$$

If $k \geq 2$, then the first six terms of (V_n) modulo 2^{k+2} are

$$2,\ P,\ -2,\ P,\ 2,\ P.$$

It follows that $V_n/P \equiv 1 \pmod 4$ if $n \equiv \pm 1 \pmod 4$ for $k \geq 1$. The result follows. □

Lemma 2.6 is due to Carmichael and follows from Theorem XI of [3].

Lemma 2.6. *Consider the Lucas sequence $V(P, Q)$, where $\gcd(P, Q) = 1$. Let p be an odd prime such that $p^i \parallel V_1$ and let $m \geq 1$ be an odd integer. Then, $p^{i+1} \mid V_m$ if and only if $p \mid m$.*

3. Proof of the Main Theorem

Proof of Theorem 1.5. We first show that we can assume that $P > 0$. We claim that the Dickson pseudoprime N with respect to $V(P, Q)$ is also a Dickson pseudoprime with respect to $V(-P, Q)$. By the recursion relation (1.2) defining $V(P, Q)$ and induction, we see that

$$V_N(-P, Q) = (-1)^N V_N(P, Q) \equiv (-1)^N P \equiv -P \pmod N,$$

and N is a Dickson pseudoprime with respect to $V(-P, Q)$. We observe that $\gcd(-P, N) = \gcd(P, N) = 1$ and $3 \nmid N$ if $-P$ is odd. We also note that $V(P, Q)$ and $V(-P, Q)$ have the same discriminant $P^2 - 4Q$. Suppose that $P > 0$ and we have proven that $m = V_N(P, Q)/P$ is a Dickson pseudoprime with respect to $V(P, Q)$ such that $\gcd(P, m) = 1$ and $3 \nmid m$ if P is odd. Then,

$$V_N(-P, Q)/(-P) = (-1)^N V_N(P, Q)/(-P) = V_N(P, Q)/P = m.$$

It now follows from our arguments above that $V_N(-P, Q)/(-P) = m$ is also a pseudoprime with respect to $V(-P, Q)$ such that $\gcd(-P, m) = 1$ and $3 \nmid m$ if $-P$ is odd. It follows that we can assume that $P > 0$ in our proof.

Because $V_1 = P$ and N is odd, it follows from Proposition 1.2 (iii) that $P \mid V_N$. By Remark 1.4 and Lemma 2.3, $D > 0$, $V_n > 0$ for $n \geq 0$, and V_n is increasing for $n \geq 1$. Let $r = V_N/P$. By our previous discussion, $r > 0$. Because N is a Dickson pseudoprime and $\gcd(N, P) = 1$, we see that $r \equiv 1 \pmod N$. We now show that r is odd and composite. If P is odd, then r is odd because $3 \nmid N$ and by Lemma 2.1 (iii). If P is even, then r is odd because N is odd and by Lemma 2.4. Because N is odd and composite, there exists an odd integer a such that $3 \leq a < N$ and a is a divisor of N. Because V_n is increasing for $n \geq 1$, $P = V_1 < V_a < V_N$. Noting that $P \mid V_a$ and $V_a \mid V_N$ by Proposition 1.2 (iii), it follows that V_N/P is composite. Moreover, $\gcd(r, P) = 1$ by Lemma 2.6, since N is odd and $\gcd(N, P) = 1$. We now demonstrate that if P is odd, then $3 \nmid r$. By assumption, $3 \nmid N$. Suppose that $3 \mid P$. Then, $3 \nmid V_N/P = r$ by Lemma 2.6. Now suppose that $3 \nmid P$. Then, $3 \nmid V_N$ by Lemma 2.2 (iv)–(vi), since N is odd. Therefore, $3 \nmid V_N/P = r$.

Let $s = (r - 1)/2 = 2^j t$, where $j \geq 0$ and t is odd. Because $r \equiv 1 \pmod N$, we observe that $N \mid 2s$. Noting that N is odd, we find that $N \mid t$. It now follows from Proposition 1.2 (iii) that

$$r = (V_N/P) \mid V_N \mid V_t. \tag{3.1}$$

First suppose that $j \geq 1$. By repeated applications of Proposition 1.2 (i), we observe that

$$U_s = U_t V_t V_{2t} \cdots V_{2^{j-1}t}, \tag{3.2}$$

which implies by (3.1) that $r \mid U_s$. Noting that s is even and $r = 2s + 1$, it follows by (3.1), (3.2), and Proposition 1.2 (iv) that

$$V_r - Q^s V_1 = V_r - P = DU_s U_{s+1} \equiv 0 \pmod{r}. \tag{3.3}$$

Hence, by (3.3), $V_r \equiv P \pmod{r}$ and $r = V_N/P$ is a Dickson pseudoprime.

Now suppose that $j = 0$. Then, $s = t$ and s is odd. Because s is odd, $r \equiv 3 \pmod 4$, which would contradict Lemma 2.5 were Q equal 1. Thus, $Q = -1$. It now follows by (3.1) and Proposition 1.2 (v) that

$$V_r + Q^s V_1 = V_r + (-1)^s P = V_r - P = V_s V_{s+1} \equiv 0 \pmod{r}. \tag{3.4}$$

Therefore by (3.4), $V_r \equiv P \pmod{r}$ and $r = V_N/P$ is again a Dickson pseudoprime. □

Acknowledgment

This paper was supported by RVO 67985840 of the Czech Republic.

References

[1] R. Baillie and S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp., **35** (1980), 1391–1417.
[2] P. S. Bruckman, *On the infinitude of Lucas pseudoprimes*, The Fibonacci Quarterly, **32.2** (1994), 153–154.
[3] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math., **15** (1913), 30–70.
[4] P. Hilton, J. Pedersen, and L. Somer, *On Lucasian numbers*, The Fibonacci Quarterly, **35.1** (1997), 43–47.
[5] F. Luca and L. Somer, *Lucas sequences for which* $4 \mid \phi(|u_n|)$ *for almost all* n, The Fibonacci Quarterly, **44.3** (2006), 249–263.
[6] A. Rotkiewicz, *On the pseudoprimes with respect to the Lucas sequence*, Bull. Acad. Polon. Sci. Sér. Math. Astronom. Phys., **21** (1973), 793–797.
[7] A. Rotkiewicz, *Lucas and Frobenius pseudoprimes* Ann. Math. Sil., **17** (2003), 17–39.
[8] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J., **21** (1954), 607–614.

MSC2020: 11B39, 11A51

Lawrence Somer, Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A.
Email address: somer@cua.edu

Michal Křížek, Institute of Mathematics, Czech Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic
Email address: krizek@math.cas.cz