ON PRIMES AND TERMS OF PRIME OR 2^k INDEX IN THE LEHMER SEQUENCES

John H. Jaroma

Department of Mathematical Sciences, Loyola College in Maryland, Baltimore, MD 21210

(Submitted May 2004-Final Revision March 2006)

ABSTRACT

It is known that with a very small number of exceptions, for a term of a Lehmer sequence $\{U_n(\sqrt{R}, Q)\}$ to be prime its index must be prime. For example, $F_4 = U_4(1, -1) = 3$ is prime. Also, $U_n(1, 2)$ is prime for $n = 6, 8, 9, 10, 15, 25, 25, 65$, while $V_n(1, 2)$ is prime for $n = 9, 12$, and 20. This criterion extends to the companion Lehmer sequences $\{V_n(\sqrt{R}, Q)\}$, with the exception that primality may occur if the index is a power of two. Furthermore, given an arbitrary prime p or any positive integer k, there does not exist an explicit means for determining whether U_p, V_p, or V_{2^k} is prime. In 2000, V. Drobot provided conditions under which if p and $2p-1$ are prime then F_p is composite. A short while later, L. Somer considered primes of the form $2p \pm 1$, as well as generalized Drobot's theorem to the Lucas sequences. Most recently, J. Jaroma extended Somer's findings to the companion Lucas sequences. In this paper, we shall generalize all of the aforementioned results from the Lucas sequences to the Lehmer sequences.

1. INTRODUCTION

In [1], V. Drobot introduced the following theorem. It gave a set of sufficient conditions for a Fibonacci number of prime index to be composite.

Theorem 1 (Drobot): Let $p > 7$ be a prime satisfying the following two conditions:

1. $p \equiv 2 \pmod 5$ or $p \equiv 4 \pmod 5$
2. $2p - 1$ is prime

Then, F_p is composite. In fact, $(2p-1) | F_p$.

In [6], L. Somer generalized the above theorem to the Lucas sequences. Let P and Q be nonzero relatively prime integers. The *Lucas sequences* $\{U_n(P, Q)\}$ are defined as

$$U_{n+2} = PU_{n+1} - QU_n, \quad U_0 = 0, \ U_1 = 1, \ n \in \{0, 1, \dots\}. \tag{1}$$

The *companion Lucas sequences* $\{V_n(P, Q)\}$ are given by

$$V_{n+2} = PV_{n+1} - QV_n, \quad V_0 = 2, \ V_1 = P, \ n \in \{0, 1, \dots\}. \tag{2}$$

Furthermore, if we let $D = P^2 - 4Q$ denote the discriminant of the characteristic equation of (1) and (2), then Somer's extension of Theorem 1 may be stated as

Theorem 2 (Somer): Let $\{U(P, Q)\}$ be a Lucas sequence and p be an odd prime such that $2p \pm 1 \nmid Q$.

1. If $2p - 1$ is a prime, $\left(\frac{D}{2p-1}\right) = -1$ and $\left(\frac{Q}{2p-1}\right) = 1$, then $2p - 1 | U_p$.
2. If $2p + 1$ is a prime, $\left(\frac{D}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = 1$, then $2p + 1 | U_p$.

Somer's result was originally given in [6, pg. 435] in terms of the second-order linear recurrence satisfying $u_{n+2} = au_{n+1} + bu_n, u_0 = 0, u_1 = 1$, and $a, b \in Z$. It was also noted in

[2] that in light of the second line of Table 1 on pg. 373 of [5], if the hypotheses of the above theorem are strengthened to include the conditions that $2p \pm 1 \not| P$ and $\gcd(P, Q) = 1$, then Theorem 2 can be reformulated to provide necessary and sufficient conditions for $2p \pm 1$ to be prime. Also, found in [2] are the following results for the companion Lucas sequences.

Theorem 3: Let $\{V(P, Q)\}$ be a companion Lucas sequence and let p be an odd prime such that $(2p \pm 1) \not| PQ$.

1. Let $\left(\frac{Q}{2p-1}\right) = \left(\frac{D}{2p-1}\right) = -1$. Then, $2p - 1 | V_p$ if and only if $2p - 1$ is prime.
2. Let $\left(\frac{Q}{2p+1}\right) = -1$ and $\left(\frac{D}{2p+1}\right) = 1$. Then, $2p + 1 | V_p$ if and only if $2p + 1$ is prime.

2. THE RESULTS

We shall now extend all of the aforementioned results to the larger family of Lehmer sequences. To this end, let p be of the arbitrary form

$$p = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \pm 1, \tag{3}$$

where, $\alpha \geq 1$, and for $1 \leq i \leq k$, $\alpha_i \in \{0, 1, \dots\}$ and the p_i are distinct odd primes. Any odd p may always be described in either of the two forms described by (3). Now, letting R and Q be any pair of relatively prime integers, the *Lehmer sequences* $\{U_n(\sqrt{R}, Q)\}$ are recursively defined as

$$U_{n+2}(R, Q) = \sqrt{R} U_{n+1} - Q U_n, \;\; U_0 = 0, \;\; U_1 = 1, \;\; n \in \{0, 1, \dots\}. \tag{4}$$

Also, the *companion Lehmer sequences* $\{V_n(\sqrt{R}, Q)\}$ are similarly given by

$$V_{n+2}(R, Q) = \sqrt{R} V_{n+1} - Q V_n, \;\; V_0 = 2, \;\; V_1 = \sqrt{R}, \;\; n \in \{0, 1, \dots\}. \tag{5}$$

As Lehmer had declared in [3], we say that m *divides* $\sqrt{R}$ *when and only when* $m^2 \mid R$. Let $\Delta = R - 4Q$ be the discriminant of the characteristic equation of (4) and (5), the following Legendre symbols will be used in this paper.

$$\sigma = \left(\frac{R}{p}\right), \qquad \tau = \left(\frac{Q}{p}\right), \qquad \epsilon = \left(\frac{\Delta}{p}\right).$$

Finally, the *rank of apparition* of a number N is the index of the first term of the underlying sequence that contains N as a factor. We shall let $\omega(p)$ represent the rank of apparition of p in $\{U_n(\sqrt{R}, Q)\}$ and $\lambda(p)$ denote the rank of apparition of p in $\{V_n(\sqrt{R}, Q)\}$. Our forthcoming generalization will require the following lemmata found in [3].

Lemma 1: $\mathrm{GCD}(U_n, V_n) = 1$ or 2.

Lemma 2: If $N \pm 1$ is the rank of apparition of N, then N is prime.

Lemma 3: If $p \not| RQ$ then $p \mid U_{p-\sigma\epsilon}$.

Lemma 4: Let $p \not| RQ$. Then, $p \mid U_{\frac{p-\sigma\epsilon}{2}}$ if and only if $\sigma = \tau$.

Lemma 5: If the rank of apparition of p, $\omega(p)$, is odd then $p \not| V_n(R, Q)$ for any value of n. If $\omega(p)$ is even, say $2k$, then $p \mid V_{(2n+1)k}$ for all n and no other term of the sequence may contain p as a factor.

Lemma 6: U_n is divisible by p if and only if $n = k\omega(p)$.

We now establish our results.

Theorem 4: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $p = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} - 1$ is prime, and $\gcd(2p+1, RQ\Delta) = 1$. For the following Jacobi symbols, let either $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = 1$ or $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = -1$. If $2p+1 = 2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} - 1$ is prime, then $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} - 1 \mid U_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1}$.

Proof: Let $2p+1 = 2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} - 1$ be prime. Now, $\sigma\epsilon = \left(\frac{R}{2p+1}\right)\left(\frac{\Delta}{2p+1}\right) = 1$. Hence, from Lemma 3, $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} - 1 \mid U_{2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-2}$. Furthermore, since $\sigma = \tau$, by Lemma 4, $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} - 1 \mid U_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1}$. $\square$

Theorem 5: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $p = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} + 1$ is prime, and $\gcd(2p-1, RQ\Delta) = 1$. For the following Jacobi symbols, let $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = 1$ or $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = -1$. If $2p-1 = 2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} + 1$ is prime, then $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} + 1 \mid U_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1}$.

Proof: Let $2p-1 = 2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} + 1$ be prime. Since $\sigma\epsilon = -1$, it follows that $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} + 1 \mid U_{2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+2}$. Finally, as $\sigma = \tau$, we have $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} + 1 \mid U_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1}$. $\square$

Let $N = q_1^{\beta_1}q_2^{\beta_2}\cdots q_r^{\beta_r}$ be any odd composite number where $q_i < q_j$ whenever $i < j$, $\gcd(N, QD) = 1$, and $U_{N-\varepsilon(N)} \equiv 0 \pmod{N}$, where $\varepsilon(N)$ denotes the Jacobi symbol, $\left(\frac{D}{N}\right)$. Then, N is a *Lucas pseudoprime for* $\{U_n(P,Q)\}$. Furthermore, N is called a *Lucas d-pseudoprime* provided that there exists a Lucas sequence $\{U_n(P,Q)\}$ satisfying $\gcd(N, PQD) = 1$, where N is a pseudoprime for $\{U_n(P,Q)\}$ and $\omega(N) = \frac{N-\varepsilon(N)}{d}$ is the rank of apparition of N in $\{U_n(P,Q)\}$. Moreover, we say that n is a *Lehmer d-pseudoprime* if there exists a Lehmer sequence $\{U_n(\sqrt{R},Q)\}$ satisfying $\gcd(N, RQ\Delta) = 1$: $\omega(N) = \frac{N-\sigma(N)\epsilon(N)}{d}$, where $\sigma(N)$ and $\epsilon(N)$ denote the Jacobi symbols (R/N) and (Δ/N), respectively. It follows from results found in [3] and from Chapter 5 in [4] that an odd composite integer N is a Lehmer d-pseudoprime if and only if it is a Lucas d-pseudoprime. Hence, If we consider the work of Somer, who in [5] showed that for any fixed d: $4 \not| d$, there exists only a finite number of Lucas d-pseudoprimes, then the statements of Theorems 4 and 5 are able to be strengthened to necessary and sufficient ones. For this purpose, we note that if $d = 2$, then the only Lucas (and hence, Lehmer) 2-pseudoprime is 3^2. This occurs, for instance, in $\{U(4,-1)\}$.

Remark 1: In [5], Somer illustrates that $N = 9$ is the only composite number for which $\omega(N) = \frac{N\pm1}{2}$. Therefore, as previously noted, $N = 9$ is the only Lehmer 2-pseudoprime. Furthermore, the rank of apparition of 9 is always equal to 4 and never equal to a prime value. This follows since $N = 9$ is a square, and so, $\sigma(N) = \epsilon(N) = 1$ whenever $\gcd(9, R\Delta) = 1$. Thus, for any Lehmer sequence in which 9 is a Lehmer 2-pseudoprime, we have $\omega(9) = \frac{9-\sigma(9)\epsilon(9)}{2} = \frac{9-1}{2} = 4$. Therefore, all other N with this particular rank of apparition must be prime.

We now restate Theorems 4 and 5 to reflect necessary and sufficient conditions for the primality of $2p \pm 1 = 2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \pm 1$. The demonstration we give for Theorem 6 is for necessity only. The sufficiency portion follows from Theorem 4. The proof of Theorem 7 is similar and omitted.

Theorem 6: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $p = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$ is prime, and $\gcd(2p+1, RQ\Delta) = 1$. Let $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = 1$ or $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = -1$. Then, $2p+1 = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$ is prime if and only if $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1 \mid U_{2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1}$.

Proof: ($\Leftarrow$) In each case, let $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1 \mid U_{2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1}$. Since the index of $U_{2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1}$ is prime and equal to $\frac{(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) - 1}{2}$, we have $\omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$. Therefore, by Remark 1, $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$ is prime. $\square$

Theorem 7: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $p = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$ is prime, and $\gcd(2p-1, RQ\Delta) = 1$. Let $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = 1$ or $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = -1$. Then, $2p-1 = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$ is prime if and only if $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1 \mid U_{2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1}$.

Theorems 6 and 7 will now be extended to the companion Lehmer sequences after offering a comment on a connection between Lehmer's original proof of the Lucas-Lehmer test given in [3] and establishing a primality test for numbers of the form $2n \pm 1$ using the companion Lehmer sequences, in general.

Remark 2: The Lucas-Lehmer test states that $2^n - 1$ *is prime if and only if* $2^n - 1$ *divides the* $(n-1)$*st term of the sequence,* 4, 14, 194, 37634, ..., S_k, ..., *where,* $S_k = S_{k-1}^2 - 2$. Equivalently, the terms of the described sequence are those of the companion Lehmer sequence $\{V_n(\sqrt{2}, 1)\}$ with indices equal to 2^k. Hence, we may restate the said result as, $2^n - 1$ *is prime if and only if* $2^n - 1 \mid V_{2^{n-1}}(\sqrt{2}, -1)$. Moreover, based on the proof of the result given in [3], we may also infer that if $n = 2^k$ for some $k \geq 1$, then $2n \pm 1$ is prime if and only if $2n \pm 1 \mid V_n$, when $\left(\frac{R}{2n\pm1}\right)\left(\frac{Q}{2n\pm1}\right) = -1$. Finally, when $n = 2^k$ and $2n \pm 1$ is a prime, then $2n \pm 1$ is either a Mersenne prime (for the case $2n-1$) or a Fermat prime (for the case $2n+1$).

Theorem 8: Let $\{V_n(\sqrt{R},Q)\}$ be a companion Lehmer sequence, $\alpha \geq 0$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$, and $\gcd(2n+1, RQ\Delta) = 1$. Let $\left(\frac{R}{2n+1}\right) = \left(\frac{\Delta}{2n+1}\right) = -\left(\frac{Q}{2n+1}\right) = 1$ or $\left(\frac{R}{2n+1}\right) = \left(\frac{\Delta}{2n+1}\right) = -\left(\frac{Q}{2n+1}\right) = -1$.

1. If n is a prime, then $2n+1 = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$ is prime if and only if $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1 \mid V_{2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1}$.
2. If $n = 2^\alpha$, then $2n+1 = 2^{\alpha+1} + 1$ is prime if and only if $2^{\alpha+1} + 1 \mid V_{2^\alpha}$.

Proof:

1. As $\sigma\epsilon = 1$, by Lemma 3, $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1 \mid U_{2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 2}$. Also, since $\sigma \neq \tau$, then $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1 \nmid U_{2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1}$. Since $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 2 = 2(2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1)$, by Lemma 6, either $\omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) = 2$ or $\omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 2$. Now, $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1 \nmid R$. So, $\omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) \neq 2$. Thus, $\omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 2$, and by Lemma 5,

$\lambda(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1) = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$. Therefore, $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1 \mid V_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1}$. Now, let $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1 \mid V_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k{\alpha_k}-1}$. Since $U_{2n}=U_nV_n$, it follows that $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1 \mid U_{2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k{\alpha_k}-2}$. By Lemma 1, $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1 \not| U_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k{\alpha_k}-1}$. So, as $\omega(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1)\neq 2$, we have $\omega(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1) = 2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-2$. Therefore, by Lemma 2, $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$ is prime.

2. Let $2m+1 = 2^{\alpha+1}+1$ be prime. As $\sigma\epsilon = 1$, by Lemma 3, $2^{\alpha+1}+1 \mid U_{2^{\alpha+1}}$. Since $\sigma\tau = -1$; that is, $\sigma \neq \tau$, we have $2^{\alpha+1}+1 \not| U_{2^{\alpha}}$. Thus, $\omega(2^{\alpha+1}+1) = 2^{\alpha+1}$ and $\lambda(2^{\alpha+1}+1) = 2^{\alpha}$. Therefore, $2^{\alpha+1}+1 \mid V_{2^{\alpha}}$. On the other hand, if $2^{\alpha+1}+1 \mid V_{2^{\alpha}}$, then by the identity $U_{2n}=U_nV_n$, it follows that $2^{\alpha+1}+1 \mid U_{2^{\alpha+1}}$. However, by Lemma 1, $2^{\alpha+1}+1 \not| U_{2^{\alpha}}$. So, $\omega(2^{\alpha+1}+1) = 2^{\alpha+1}$. Therefore, by Lemma 2, $2^{\alpha+1}+1$ is prime. □

Theorem 9: Let $\{V_n(\sqrt{R},Q)\}$ be a companion Lehmer sequence, $\alpha \geq 0$, for $1\leq i\leq k$ assume that $\alpha_i \geq 0$, $n = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1$, and $\gcd(2n+1, RQ\Delta)=1$. Let $\left(\frac{R}{2n-1}\right) = -\left(\frac{\Delta}{2n-1}\right) = -\left(\frac{Q}{2n-1}\right) = 1$ or $\left(\frac{R}{2n-1}\right) = -\left(\frac{\Delta}{2n-1}\right) = -\left(\frac{Q}{2n-1}\right) = -1$.

1. If n is a prime, then $2n-1 = 2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1$ is prime if and only if $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1 \mid V_{2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1}$.

2. If $n = 2^{\alpha}$, then $2n-1 = 2^{\alpha+1}-1$ is prime if and only if $2^{\alpha+1}-1 \mid V_{2^{\alpha}}$.

3. A RANK OF APPARITION INTERPRETATION

We say that p has *maximal rank of apparition* in $\{U_n(\sqrt{R},Q)\}$ provided that $\omega(p) = p\pm 1$. If p divides the term, say U_q, where q is a prime, then we may necessarily conclude that $\omega(p) = q$. As a result, Theorems 4 through 9 are easily restated in order that each may provide a rank of apparition result. Theorems 8A and 9A provide maximal rank of apparition results.

Theorem 4A: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1\leq i\leq k$ assume that $\alpha_i \geq 0$, $p = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$ is prime, and $\gcd(2p+1, RQ\Delta)=1$. Let either $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = 1$ or $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = -1$. If $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$ is prime, then $\omega(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1) = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$ and $\lambda(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1)$ does not exist.

Theorem 5A: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1\leq i\leq k$ assume that $\alpha_i \geq 0$, $p = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1$ is prime and $\gcd(2p-1, RQ\Delta)=1$. Let $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = 1$ or $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = -1$. If $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1$ is prime, then $\omega(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1) = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1$ and $\lambda(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}+1)$ does not exist.

Theorem 6A: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1\leq i\leq k$ assume that $\alpha_i \geq 0$, $p = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$ is prime, and $\gcd(2p+1, RQ\Delta)=1$. Let $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = 1$ or $\left(\frac{R}{2p+1}\right) = \left(\frac{\Delta}{2p+1}\right) = \left(\frac{Q}{2p+1}\right) = -1$. Then, $2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$ is prime $\Longleftrightarrow \omega(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1) = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1$ and $\lambda(2^{\alpha+1}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}-1)$ does not exist.

Theorem 7A: Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence, $\alpha \geq 1$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $p = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$ is prime, and $\gcd(2p-1, RQ\Delta) = 1$. Let $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = 1$ or $\left(\frac{R}{2p-1}\right) = -\left(\frac{\Delta}{2p-1}\right) = \left(\frac{Q}{2p-1}\right) = -1$. Then, $2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$ is prime $\Longleftrightarrow \omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1) = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$ and $\lambda(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1)$ does not exist.

Theorem 8A: Let $\{V_n(\sqrt{R},Q)\}$ be a companion Lehmer sequence, $\alpha \geq 0$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$, and $\gcd(2n+1, RQ\Delta) = 1$. Also, let $\left(\frac{R}{2n+1}\right) = \left(\frac{\Delta}{2n+1}\right) = -\left(\frac{Q}{2n+1}\right) = 1$ or $\left(\frac{R}{2n+1}\right) = \left(\frac{\Delta}{2n+1}\right) = -\left(\frac{Q}{2n+1}\right) = -1$.

1. If n is a prime, then $2n+1 = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$ is prime $\Longleftrightarrow \omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 2$ and $\lambda(2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1) = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} - 1$.
2. If $n = 2^\alpha$, then $2n+1 = 2^{\alpha+1}+1$ is prime $\Longleftrightarrow \omega(2^{\alpha+1}+1) = 2^{\alpha+1}$ and $\lambda(2^{\alpha+1}+1) = 2^\alpha$.

Theorem 9A: Let $\{V_n(\sqrt{R},Q)\}$ be a companion Lehmer sequence, $\alpha \geq 0$, for $1 \leq i \leq k$ assume that $\alpha_i \geq 0$, $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$, and $\gcd(2n+1, RQ\Delta) = 1$. Also, let $\left(\frac{R}{2n-1}\right) = -\left(\frac{\Delta}{2n-1}\right) = -\left(\frac{Q}{2n-1}\right) = 1$ or $\left(\frac{R}{2n-1}\right) = -\left(\frac{\Delta}{2n-1}\right) = -\left(\frac{Q}{2n-1}\right) = -1$.

1. If n is a prime, then $2n-1 = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$ is prime $\Longleftrightarrow \omega(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1) = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 2$ and $\lambda(2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1) = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} + 1$.
2. If $n = 2^\alpha$, then $2n-1 = 2^{\alpha+1}-1$ is prime $\Longleftrightarrow \omega(2^{\alpha+1}-1) = 2^{\alpha+1}$ and $\lambda(2^{\alpha+1}-1) = 2^\alpha$.

ACKNOWLEDGMENT

The author would like to thank an anonymous referee whose careful reading of the manuscript, insight, and expertise led to many improvements in this paper, among which included the strengthening of Theorems 8, 8A, 9, 9A to the case of V_n when $n = 2^k$ and the extension of Theorems 6, 6A, 7, 7A to the Lehmer sequences.

REFERENCES

[1] V. Drobot. "On Primes in the Fibonacci Sequence." *Fibonacci Quarterly* **38** (2000): 71-72.

[2] J. H. Jaroma. "Extension of a Theorem of Somer to the Companion Lucas Sequences." *Proceedings of the 11th Conference of Fibonacci Numbers and their Applications.* Kluwer, The Netherlands, 2006, pp. 131-136.

[3] D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. Math.*, Second Series **31** (1930): 419-448.

[4] L. Somer. "The Divisibility and Modular Properties of kth-Order Linear Recurrences Over the Ring of Integers of an Algebraic Number Field With Respect to Prime Ideals." Ph.D. Dissertation, The University of Illinois at Urbana-Champaign, 1985.

[5] L. Somer. "On Lucas d-Pseudoprimes." *Fibonacci Numbers and Their Applications.* **7**: 369–375. Ed. G. E. Bergum et al. Dordrecht: Kluwer Academic Publishers, 1998.

[6] L. Somer. "Generalization of a Theorem of Drobot." *Fibonacci Quarterly* **40** (2002): 435-437.

AMS Classification Numbers: 11A51, 11B39

✠ ✠ ✠