ON THE APPEARANCE OF PRIMES IN LINEAR RECURSIVE SEQUENCES

JOHN H. JAROMA

We present an application of difference equations to number theory by considering the set of linear second-order recursive relations, $U_{n+2}(\sqrt{R}, Q) = \sqrt{R}U_{n+1} - QU_n$, $U_0 = 0$, $U_1 = 1$, and $V_{n+2}(\sqrt{R}, Q) = \sqrt{R}V_{n+1} - QV_n$, $V_0 = 2$, $V_1 = \sqrt{R}$, where R and Q are relatively prime integers and $n \in \{0, 1, \ldots\}$. These equations describe the set of extended Lucas sequences, or rather, the Lehmer sequences. We add that the *rank of apparition* of an odd prime p in a specific Lehmer sequence is the index of the first term that contains p as a divisor. In this paper, we obtain results that pertain to the rank of apparition of primes of the form $2^n p \pm 1$. Upon doing so, we will also establish rank of apparition results under more explicit hypotheses for some notable special cases of the Lehmer sequences. Presently, there does not exist a closed formula that will produce the rank of apparition of an arbitrary prime in any of the aforementioned sequences.

1. Introduction

Linear recursive equations such as the family of second-order extended Lucas sequences described above have attracted considerable theoretic attention for more than a century. Among other things, they have played an important role in primality testing. For example, the prime character of a number is often a consequence of having *maximal rank of apparition*; that is, rank of apparition equal to $N \pm 1$.

The first objective of this paper is to provide a general rank-of-apparition result for primes of the form $N = 2^n p \pm 1$, where p is a prime. Then, using more explicit criteria, we will determine when such primes have maximal rank of apparition in the specific Lehmer sequences $\{F_n\} = \{U_n(1, -1)\} = \{1, 1, 2, 3, \ldots\}$ and $\{L_n\} = \{V_n(1, -1)\} = \{1, 3, 4, 7, \ldots\}$. Respectively, $\{F_n\}$ and $\{L_n\}$ represent the Fibonacci and the Lucas numbers.

2. The Lucas and Lehmer sequences

In [4], Lucas published the first set of papers that provided an in-depth analysis of the numerical factors of the set of sequences generated by the second-order linear recurrence relation $X_{n+2} = PX_{n+1} - QX_n$, where $n \in \{0, 1, \ldots\}$ [4]. These sequences also attracted the attention of P. de Fermat, J. Pell, and L. Euler years earlier. Nevertheless, it was Lucas

who undertook the first systematic study of them. In 1913, Carmichael introduced some corrections to Lucas's papers, and also generalized some of the results [1, 2].

We now define the Lucas sequences. Let P and Q be any pair of nonzero relatively prime integers. Then, the *Lucas sequences* $\{U_n(P,Q)\}$ and the *companion Lucas sequences* $\{V_n(P,Q)\}$ are recursively given by

$$
\begin{aligned}
U_{n+2} &= PU_{n+1} - QU_n, \quad U_0 = 0, \quad U_1 = 1, \quad n \in \{0,1,2,\dots\}, \\
V_{n+2} &= PV_{n+1} - QV_n, \quad V_0 = 2, \quad V_1 = P, \quad n \in \{0,1,2,\dots\}.
\end{aligned}
\tag{2.1}
$$

In [3], Lehmer extended the theory of the Lucas functions to a more general class of sequences described by replacing the parameter P in (2.1) with $\sqrt{R}$ under the assumption that R and Q are relatively prime integers. In particular, the *Lehmer sequences* $\{U_n(\sqrt{R},Q)\}$ and the *companion Lehmer sequences* $\{V_n(\sqrt{R},Q)\}$ are defined as

$$
U_{n+2}(\sqrt{R},Q) = \sqrt{R}U_{n+1} - QU_n, \quad U_0 = 0, \quad U_1 = 1, \quad n \in \{0,1,\dots\},
\tag{2.2}
$$

$$
V_{n+2}(\sqrt{R},Q) = \sqrt{R}V_{n+1} - QV_n, \quad V_0 = 2, \quad V_1 = \sqrt{R}, \quad n \in \{0,1,\dots\}.
\tag{2.3}
$$

We remark that Lehmer's modification of the Lucas sequences shown in (2.2) and (2.3) was motivated by the fact that the discriminant $P^2 - 4Q$ of the characteristic equation of (2.1) cannot be of the form $4k + 2$ or $4k + 3$.

3. Properties of the Lehmer sequences

Throughout the rest of this paper, p will denote an odd prime. In addition, we also adopt the notation $\omega(p)$ and $\lambda(p)$ to describe, respectively, the rank of apparition of p in $\{U_n\}$ and in $\{V_n\}$. Furthermore, if $\omega(p) = n$, then p is called a *primitive prime factor* of U_n. Similarly, if $\lambda(p) = n$, then p is said to be a primitive prime factor of V_n. Finally, (a/p) shall denote the Legendre symbol of p and a. We now introduce some divisibility characteristics of the Lehmer sequences [3].

LEMMA 3.1. *Let $p \nmid RQ$. Then, $U_{p-\sigma\epsilon}(\sqrt{R},Q) \equiv 0 \pmod{p}$.*

LEMMA 3.2. *$p \mid U_n(\sqrt{R},Q)$ if and only if $n = k\omega$.*

LEMMA 3.3. *Suppose that $\omega(p)$ is odd. Then $V_n(\sqrt{R},Q)$ is not divisible by p for any value of n. On the other hand, if $\omega(p)$ is even, say $2k$, then $V_{(2n+1)k}(\sqrt{R},Q)$ is divisible by p for every n but no other term of the sequence may contain p as a factor.*

LEMMA 3.4. *Let $p \nmid RQ$. Then, $U_{(p-\sigma\epsilon)/2}(\sqrt{R},Q) \equiv 0 \pmod{p}$ if and only if $\sigma = \tau$.*

LEMMA 3.5. *Let $p \nmid RQ$. If $p \mid Q$. Then $p \nmid U_n$, for all n. If $p^2 \mid R$, then $\omega(p) = 2$. If $p \mid \Delta$, then $\omega(p) = p$.*

4. Rank of apparition of a prime of the form $2^n p \pm 1$ in $\{U_n\}$ and $\{V_n\}$

We now introduce the Legendre symbols $\sigma = (R/p), \tau = (Q/p)$, and $\epsilon = (\Delta/p)$, where $\Delta = R - 4Q$ is the discriminant of the characteristic equation of (2.2) and (2.3). The following

two theorems pertain to the rank of apparition of a prime of the form $2^n p \pm 1$ in the Lehmer sequences. Because of Lemma 3.5, we impose the restriction $q \nmid RQ\Delta$.

Theorem 4.1. *Let $q = 2^n p - 1$ be prime and $q \nmid RQ\Delta$. Also, assume that either $\sigma = 1$, $\epsilon = -1$, $\tau = -1$ or $\sigma = -1$, $\epsilon = 1$, $\tau = 1$.*

  (1) *If $n = 1$, then $\omega(q) = 2p$ and $\lambda(q) = p$.*
  (2) *If $n > 1$ and $q \mid V_{2^{n-1}}(\sqrt{R}, Q)$, then $\omega(q) = 2^n$ and $\lambda(q) = 2^{n-1}$.*
  (3) *If $n > 1$ and $q \nmid V_{2^{n-1}}(\sqrt{R}, Q)$, then $\omega(q) = 2^n p$ and $\lambda(q) = 2^{n-1} p$.*

Proof. In each case, $\sigma\epsilon = -1$. So, by Lemma 3.1, $q \mid U_{2^n p}$. Furthermore, since $\sigma \neq \tau$, it follows by Lemma 3.4 that $q \nmid U_{2^{n-1} p}$. Hence, by Lemma 3.2, the only possible values for $\omega(q)$ are 2^n and $2^n p$.

  (1) Let $n = 1$. Thus, either $\omega(q) = 2$ or $\omega(q) = 2p$. However, by (2.2), we see that $U_2 = \sqrt{R} U_1 - Q U_0 = \sqrt{R} \cdot 1 - Q \cdot 0 = \sqrt{R}$. Furthermore, as $q^2 \nmid R$ by hypothesis, we conclude that $\omega(q) = 2p$. Finally, by Lemma 3.3, $\lambda(q) = p$.

  (2) Let $n > 1$ and $q \mid V_{2^{n-1}}$. Since $q \mid V_{2^{n-1}}$, then because of Lemma 3.3, we infer that q is a primitive prime factor of $V_{2^{n-1}}$. Hence, $\lambda(q) = 2^{n-1}$. Also, by the same lemma, this can happen only if $\omega(q) = 2^n$.

  (3) Let $n > 1$ and $q \nmid V_{2^{n-1}}$. Then, $\lambda(q) \neq 2^{n-1}$. By Lemma 3.3, this means that $\omega(q) \neq 2^n$. Thus, the only choice for $\omega(q)$ is $2^n p$. Therefore, $\lambda(q) = 2^{n-1} p$. □

Theorem 4.2. *Let $q = 2^n p + 1$ be prime and $q \nmid RQ\Delta$. Also, assume that either $\sigma = 1$, $\epsilon = 1$, $\tau = -1$ or $\sigma = -1$, $\epsilon = -1$, $\tau = 1$.*

  (1) *If $n = 1$, then $\omega(q) = 2p$ and $\lambda(q) = p$.*
  (2) *If $n > 1$ and $q \mid V_{2^{n-1}}(\sqrt{R}, Q)$, then $\omega(q) = 2^n$ and $\lambda(q) = 2^{n-1}$.*
  (3) *If $n > 1$ and $q \nmid V_{2^{n-1}}(\sqrt{R}, Q)$, then $\omega(q) = 2^n p$ and $\lambda(q) = 2^{n-1} p$.*

Proof. In all three cases, we see that $\sigma\epsilon = 1$. Hence, $q \mid U_{2^n p}$. In addition, $\sigma \neq \tau$. So, it follows by Lemma 3.4 that $q \nmid U_{2^{n-1} p}$. Thus, the only possible values for $\omega(q)$ are 2^n and $2^n p$.

  (1) Let $n = 1$. Then, either $\omega(q) = 2$ or $\omega(q) = 2p$. However, from (2.2), $U_2 = \sqrt{R} U_1 - Q U_0 = \sqrt{R} \cdot 1 - Q \cdot 0 = \sqrt{R}$. Since $q \nmid \sqrt{R}$ by hypothesis, we conclude that $\omega(q) = 2p$ and $\lambda(q) = p$.

  (2) Let $n > 1$ and $q \mid V_{2^{n-1}}(\sqrt{R}, Q)$. Using an argument similar to the one given in the second part of Theorem 4.1, we have $\omega(q) = 2^n$ and $\lambda(q) = 2^{n-1}$.

  (3) Let $n > 1$ and $q \nmid V_{2^{n-1}}(\sqrt{R}, Q)$. Similarly, by an argument analogous to the one provided in the third part of Theorem 4.1, it follows that $\omega(q) = 2^n p$ and $\lambda(q) = 2^{n-1} p$. □

5. Explicit results for primes of the form $2^n p \pm 1$ in $\{F_n\}$ and $\{L_n\}$

In this section, we obtain explicit results for the rank of apparition of a prime of the form $2^n p \pm 1$ in the sequences of Fibonacci and Lucas numbers. In both sequences, $R = -Q = 1$ and $\Delta = R - 4Q = 5$.

First, in the following category of primes, we identify values for p and n under which $\epsilon = (\Delta/(2^n p - 1)) = (5/(2^n p - 1)) = -1$. Shortly thereafter, we consider a second category that will allow us to accomplish a similar objective for primes of the form $2^n p + 1$.

Prime Category I.

$$p \equiv 1 (\mathrm{mod}\, 5), \quad \text{and either} \quad n \equiv 2 (\mathrm{mod}\, 4) \quad \text{or} \quad n \equiv 3 (\mathrm{mod}\, 4).$$
$$p \equiv 2 (\mathrm{mod}\, 5), \quad \text{and either} \quad n \equiv 1 (\mathrm{mod}\, 4) \quad \text{or} \quad n \equiv 2 (\mathrm{mod}\, 4).$$
$$p \equiv 3 (\mathrm{mod}\, 5), \quad \text{and either} \quad n \equiv 0 (\mathrm{mod}\, 4) \quad \text{or} \quad n \equiv 3 (\mathrm{mod}\, 4).$$
$$p \equiv 4 (\mathrm{mod}\, 5), \quad \text{and either} \quad n \equiv 0 (\mathrm{mod}\, 4) \quad \text{or} \quad n \equiv 1 (\mathrm{mod}\, 4).$$
(5.1)

LEMMA 5.1. *Let $q = 2^n p - 1$ be prime. Then, for any p, n belonging to Prime Category I, it follows that $\epsilon = (5/q) = -1$.*

Proof. Since 5 and q are distinct odd primes, both Legendre symbols $(5/q)$ and $(q/5)$ are defined.

By Gauss's reciprocity law,

$$\left(\frac{5}{q}\right)\left(\frac{q}{5}\right) = (-1)^{((5-1)/2)\cdot((q-1)/2)} = (-1)^{2(2^{n-1}p-1)} = 1.$$
(5.2)

Hence,

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right).$$
(5.3)

We now prove the first two cases of **Lemma 5.1**. The remaining two cases follow similarly, and are omitted.

(1) Suppose that $p \equiv 1 (\mathrm{mod}\, 5)$, and either $n \equiv 2 (\mathrm{mod}\, 4)$ or $n \equiv 3 (\mathrm{mod}\, 4)$.
If $n = 4r + 2$, then

$$\left(\frac{5}{q}\right) = \left(\frac{2^{4r+2}(5k+1)-1}{5}\right) = \left(\frac{3}{5}\right) = -1.$$
(5.4)

If $n = 4r + 3$, then

$$\left(\frac{2^{4r+3}(5k+1)-1}{5}\right) = \left(\frac{2}{5}\right) = -1.$$
(5.5)

(2) Suppose that $p \equiv 2 (\mathrm{mod}\, 5)$, and either $n \equiv 1 (\mathrm{mod}\, 4)$ or $n \equiv 2 (\mathrm{mod}\, 4)$.
If $n = 4r + 1$, then

$$\left(\frac{2^{4r+1}(5k+2)-1}{5}\right) = \left(\frac{3}{5}\right) = -1.$$
(5.6)

If $n = 4r + 2$, then

$$\left(\frac{2^{4r+2}(5k+2)-1}{5}\right) = \left(\frac{2}{5}\right) = -1.$$
(5.7)

$\square$

We now identify values of p and n for which $\epsilon = (\Delta/(2^n p + 1)) = (5/(2^n p + 1)) = 1$.

Prime Category II.

$$p \equiv 1 \pmod 5 \quad \text{and} \quad n \equiv 3 \pmod 4.$$
$$p \equiv 2 \pmod 5 \quad \text{and} \quad n \equiv 2 \pmod 4.$$
$$p \equiv 3 \pmod 5 \quad \text{and} \quad n \equiv 0 \pmod 4. \tag{5.8}$$
$$p \equiv 4 \pmod 5, \quad \text{and either} \quad n \equiv 1 \pmod 4 \quad \text{or} \quad n \equiv 0 \pmod 4.$$

We demonstrate the first two cases and omit the last two.

Lemma 5.2. *Let $q = 2^n p + 1$ be prime. Then, for any p, n belonging to Prime Category II, it follows that $\epsilon = (5/q) = 1$.*

Proof. Using Gauss's reciprocity law, it is easily shown that $(5/q) = (q/5)$. Hence, we have the following.
(1) If $p \equiv 1 \pmod 5$ and $n \equiv 3 \pmod 4$, then

$$\left(\frac{5}{q}\right) = \left(\frac{2^{4r+3}(5k+1)+1}{5}\right) = \left(\frac{4}{5}\right) = 1. \tag{5.9}$$

(2) If $p \equiv 2 \pmod 5$ and $n \equiv 2 \pmod 4$, then

$$\left(\frac{2^{4r+2}(5k+2)+1}{5}\right) = \left(\frac{4}{5}\right) = 1. \tag{5.10}$$

$\square$

Before we establish more explicit criteria for the rank of apparition of p in either $\{F_n\}$ or $\{L_n\}$, the next two propositions are needed.

Lemma 5.3. *Let $q = 2^n p - 1$ be prime. If $n = 1$, then $\tau = (-1/q) = 1$. Otherwise, $\tau = -1$.*

Proof. Observe that

$$\left(\frac{Q}{q}\right) = \left(\frac{-1}{q}\right) \equiv (-1)^{(q-1)/2} \equiv (-1)^{2^{n-1}p-1} \pmod q. \tag{5.11}$$

First, let $n = 1$. Then, since $p - 1$ is even, it follows that $\tau = (-1/q) \equiv 1$. On the other hand, if $n > 1$, then $2^{n-1}p - 1$ is odd. Therefore, $\tau = (-1/q) = -1$. $\square$

Lemma 5.4. *Let $q = 2^n p + 1$ be prime. If $n = 1$, then $\tau = (Q/q) = (-1/q) = -1$. Otherwise, $\tau = 1$.*

Proof. First, we see that

$$\left(\frac{Q}{q}\right) = \left(\frac{-1}{q}\right) \equiv (-1)^{(q-1)/2} \equiv (-1)^{2^{n-1}p} \pmod q. \tag{5.12}$$

If $n = 1$, then $2^{n-1}p = p$. Thus, $\tau = (-1/q) = -1$. Otherwise, $2^{n-1}p$ is even, and $\tau = (-1/q) = 1$. $\square$

We now state and prove our two main results.

Theorem 5.5. *Let $q = 2^n p - 1$ be prime. Then, for any p belonging to Prime Category I such that $q \nmid 5$, the following is true regarding the rank of apparition of q in $\{F_n\}$ and $\{L_n\}$:*

(1) *if $n = 1$, then $\omega(q) = p$ and $\lambda(q)$ does not exist;*
(2) *if $n > 1$ and $q \mid L_{2^{n-1}}$, then $\omega(q) = 2^n$ and $\lambda(q) = 2^{n-1}$;*
(3) *if $n > 1$ and $q \nmid L_{2^{n-1}}$, then $\omega(q) = 2^n p$ and $\lambda(q) = 2^{n-1}p$.*

Proof. As p belongs to Prime Category I, we have by Lemma 5.1 that $\epsilon = (5/q) = -1$. Furthermore, $\sigma = (1/q) = 1$.

(1) If $n = 1$, then $q = 2p - 1$. Since $\sigma\epsilon = -1$, it follows by Lemma 3.1 that $q \mid F_{2p}$. Also, by Lemma 5.3, we have $\tau = 1$. Hence, $\sigma = \tau$. Thus, by Lemma 3.4, $q \mid F_p$. Furthermore, as every factor of F_p is primitive, it follows that $\omega(q) = p$. Finally, because $\omega(q)$ is odd, then by Lemma 3.3, q divides no term of $\{L_n\}$; that is, the rank of apparition of q in $\{L_n\}$ does not exist.

(2) Let $n > 1$ and $q \mid L_{2^{n-1}}$. Since $\sigma\epsilon = -1$, then by Lemma 3.1, it follows that $q \mid F_{2^n p}$. In addition, by Lemma 5.3, we see that $\tau = -1$. Hence, $\sigma \neq \tau$. This implies, using Lemma 3.4, that $q \nmid F_{2^{n-1}p}$. Thus, from Lemma 3.2, the only possible values for $\omega(q)$ are 2^n and $2^n p$. However, by hypothesis, $q \mid L_{2^{n-1}}$. Therefore, by Lemma 3.3, this can occur only if $\omega(q) = 2^n$ and $\lambda(q) = 2^{n-1}$.

(3) Let $n > 1$ and $q \nmid L_{2^{n-1}}$. Then, by Lemma 3.1, $q \mid F_{2^n p}$. However, by Lemma 3.4, $q \nmid F_{2^{n-1}p}$. This implies that either $\omega(q) = 2^n$ or $\omega(q) = 2^n p$. Now, by hypothesis, $q \nmid L_{2^{n-1}}$. Thus, since $q \nmid L_{2^{n-1}}$, we conclude by Lemma 3.3 that $\omega(q) \neq 2^n$. Therefore, $\omega(q) = 2^n p$ and $\lambda(q) = 2^{n-1}p$. □

Theorem 5.6. *Let p be an odd prime such that $q = 2^n p + 1$ is prime. Then, for any p belonging to Prime Category II such that $q \nmid 5$, the following is true regarding the rank of apparition of q in $\{F_n\}$ and $\{L_n\}$:*

(1) *if $n = 1$, then $\omega(q) = 2p$ and $\lambda(q) = p$;*
(2) *if $n > 1$ and $q \mid L_{2^{n-2}}$, then $\omega(q) = 2^{n-1}$ and $\lambda(q) = 2^{n-2}$.*

Proof. Since p belongs to Prime Category II, we see by Lemma 5.2 that $\epsilon = (5/q) = 1$. Also, $\sigma = (R/q) = (1/q) = 1$.

(1) If $n = 1$, then $q = 2p + 1$. Now, because $\sigma\epsilon = 1$, Lemma 3.1 tells us that $q \mid F_{2p}$. In addition, by Lemma 5.4, we have $\tau = -1$. So, $\sigma \neq \tau$. Thus, by Lemma 3.4, $q \nmid F_p$. Therefore, in light of Lemma 3.2, either $\omega(q) = 2$ or $\omega(q) = 2p$. However, by (2.2), $F_2 = \sqrt{R} = 1$. Hence, $q \nmid F_2$. Therefore, $\omega(q) = 2p$ and $\lambda(q) = p$.

(2) Let $n > 1$ and $q \mid L_{2^{n-2}}$. Since $\sigma\epsilon = 1$, by Lemma 3.1, it follows that $q \mid F_{2^n p}$. Also, by Lemma 5.4, $\tau = 1$. Hence, $\sigma = \tau$. This implies by Lemma 3.4 that $q \mid F_{2^{n-1}p}$. Thus, from Lemma 3.2, it follows that $\omega(q)$ is a divisor of $2^{n-1}p$. Moreover, by hypothesis, $q \mid L_{2^{n-2}}$. So, applying Lemma 3.3, we conclude that q can divide no term of $\{L_n\}$ with index less than 2^{n-2}. Therefore, $\lambda(q) = 2^{n-2}$, which can happen only if $\omega(q) = 2^{n-1}$. □

Remark 5.7. The case $n > 1$ and $q \nmid L_{2^{n-2}}$ was not considered. Had it been, we would have been led to the conclusion that $\omega(q) \neq 2^{n-1}$. But by Lemma 3.2, we would not be able to identify $\omega(q)$, since all of the factors of the index $2^{n-1}p$ not equal to 2 would still remain as candidates for the rank of apparition of q in $\{F_n\}$.

Acknowledgment

References

[1]   R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2) **15** (1913/1914), no. 1–4, 30–48.

[2]   ──────, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. (2) **15** (1913/1914), no. 1–4, 49–70.

[3]   D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419–448.

[4]   É. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321 (French).

John H. Jaroma: Department of Math & Computer Science, Austin College, Sherman, TX 75090, USA

E-mail address: jjaroma@austincollege.edu