Primes of the form $2^\alpha p \pm 1$ with maximal rank of apparition in the Lehmer sequences

John H. Jaroma

Abstract

The *rank of apparition* of a prime q in a given Lehmer sequence is the index of the first term in which q occurs as a divisor. Furthermore, q is said to have *maximal rank of apparition* in an underlying Lehmer sequence provided that its rank of apparition is $q \pm 1$. Letting p be a prime, in this paper we identify all primes of the form $2^\alpha p \pm 1$ that have maximal rank of apparition in the noted sequences.

1 Introduction

In 1878, É. Lucas published a seminal set of papers that studied in detail, the factors of the sequences produced by the second-order linear recurrence relation

$$U_{n+2} = PU_{n+1} - QU_n, \quad n \in \{0, 1, \ldots\}, \tag{1}$$

where P and Q are any pair of nonzero integers [3]. Important findings pertaining to the rank of apparition of a prime in sequences described by (1) were first introduced by Lucas but some of his findings contained mistakes. In 1913, R. D. Carmichael sought to correct Lucas' discrepancies and offered generalizations of his work [1]. In 1930, D. H. Lehmer further extended the results of Lucas and Carmichael to the general class of sequences that now bear his name [2]. In doing so, he also rendered the discouraging remark that an explicit formula for the rank of apparition of p "is not to be expected any more than a formula for the exponent to which a given number c belongs modulo p." Some fifty years later, L. Somer noted that the two most important questions regarding the Lucas sequences (and so arguably, the Lehmer sequences) are [4]:

Received by the editors October 2010.
Communicated by A. Weiermann.
2000 *Mathematics Subject Classification* : 11A51, 11B39.

1. Which odd primes have maximal rank of apparition?

2. For which odd prime p does a given Lucas sequence have a *maximal period modulo p*? (The period modulo p of the Lucas sequence, U_n, is the first positive integer n in which $U_n \equiv 0 \pmod{p}$ and $U_{n+1} \equiv U_1 \equiv 1 \pmod{p}$.)

Let R and Q be relatively prime integers. Then, the *Lehmer sequences* $\{U_n(\sqrt{R}, Q)\}$ are recursively defined as

$$U_{n+2} = \sqrt{R}U_{n+1} - QU_n, \;\; U_0 = 0, \;\; U_1 = 1, \;\; n \geq 0\}. \tag{2}$$

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

$$V_{n+2} = \sqrt{R}V_{n+1} - QV_n, \;\; V_0 = 2, \;\; V_1 = \sqrt{R}, \;\; n \geq 0\}. \tag{3}$$

2 Divisibility properties of the Lehmer sequences

Throughout the remainder of this paper, we let q and p denote odd primes. The following describe divisibility properties associated with the Lehmer sequences are found in [2].

Lemma 1: *Let q be an odd prime such that $q \mid Q$. Then, no term of $\{U_n(\sqrt{R}, Q)\}$ contains q as a factor.*

We now introduce the following Legendre symbols:

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

The next lemma asserts that either $q|U_{q-1}$ or $q|U_{q+1}$.

Lemma 2: *Suppose $q \nmid RQ$. Then, $q|U_{q-\sigma\epsilon}$.*

The subsequent notation is used to describe the rank of apparition of q in either the Lehmer or companion Lehmer sequences.

$$\omega(q) = \text{rank of apparition of } q \text{ in } \{U_n\}$$

$$\lambda(q) = \text{rank of apparition of } q \text{ in } \{L_n\}.$$

Lemma 3: *$q|U_n$ if and only if $n = k\omega(q)$, where k is any nonnegative integer.*

The next result tells us when q has rank of apparition in a companion Lehmer sequence.

Lemma 4: *If $\omega(q)$ is odd, then V_n is not divisible by q for any value of n. However, if for some positive integer k, $\omega(q) = 2k$, then $q|V_{(2n+1)k}$ for all n, but no other term of the sequence contains q as a factor.*

3 primes with maximal rank of apparition in the Lehmer sequences

We are now ready to address the question of which odd primes of the form $2^\alpha p \pm 1$ have maximal rank of apparition in the Lehmer sequences. To this end, we add the following important result that too originates from the work of Lehmer in [2].

Lemma 5: *Let $q \nmid RQ$. Then, $U_{\frac{q-\sigma\epsilon}{2}}(\sqrt{R}, Q) \equiv 0 \pmod{q}$ if and only if $\sigma = \tau$.*

In order to arrive at our objective, we observe that by Remark 1 and Lemma 5, the only primes we must consider are those that satisfy either (4) or (5) if q is of the form $2^\alpha p - 1$ and those that satisfy (5) or (6) when q is of the form $2^\alpha p + 1$.

$$\sigma = \left(\frac{R}{2^\alpha p - 1}\right) = 1, \quad \epsilon = \left(\frac{\Delta}{2^\alpha p - 1}\right) = -1, \quad \tau = \left(\frac{Q}{2^\alpha p - 1}\right) = -1 \tag{4}$$

$$\sigma = \left(\frac{R}{2^\alpha p - 1}\right) = -1, \quad \epsilon = \left(\frac{\Delta}{2^\alpha p - 1}\right) = 1, \quad \tau = \left(\frac{Q}{2^\alpha p - 1}\right) = 1. \tag{5}$$

$$\sigma = \left(\frac{R}{2^\alpha p + 1}\right) = 1, \quad \epsilon = \left(\frac{\Delta}{2^\alpha p + 1}\right) = 1, \quad \tau = \left(\frac{Q}{2^\alpha p + 1}\right) = -1 \tag{6}$$

$$\sigma = \left(\frac{R}{2^\alpha p + 1}\right) = -1, \quad \epsilon = \left(\frac{\Delta}{2^\alpha p + 1}\right) = -1, \quad \tau = \left(\frac{Q}{2^\alpha p + 1}\right) = 1. \tag{7}$$

We now arrive at the two rank of apparition propositions:

Theorem 1: *Let $q = 2^\alpha p - 1$, $\alpha \geq 1$, be any prime that satisfies either (4) or (5) and let $q \nmid RQ\Delta$. Then, $\omega(q) = 2^\alpha p$ and $\lambda(q) = 2^{\alpha-1} p$ if and only if $q \nmid V_{2^{\alpha-1}}(\sqrt{R}, Q)$.*

Proof. First, we note that if $q \mid \Delta$, then $(\Delta/q) = 0$. Hence, $q \mid U_q$ and the rank of apparition of q is q. Thus, q does not have maximal rank of apparition by definition. Furthermore, if $q \mid Q$, then by Lemma 1 no term of the sequence is divisible by q. Also, if $q \mid \sqrt{R}$, then in light of (2), $U_2 = \sqrt{R}$. So, the rank of apparition of q is 2 and we conclude that the only primes that are potential candidates for maximal rank of apparition in the Lehmer sequences are those that satisfy $q \nmid \sqrt{R}Q\Delta$, which is given by the statement $q \nmid RQ\Delta$. ($\Longrightarrow$) Let $\omega(q) = 2^\alpha p$. (Thus, $\lambda(q) = 2^{\alpha-1} p$ by Lemma 4.) So, $q \nmid V_{2^{\alpha-1}}(\sqrt{R}, Q)$. ($\Longleftarrow$) By Lemma 2, $q | U_{q-(\Delta/q)}$. Hence, $q | U_{2^\alpha p}$. Furthermore, by Lemma 3, the rank of apparition of q is a divisor of the index $2^\alpha p$. But by Lemma 5, $q \nmid U_{2^{\alpha-1} p}$. Hence, either $\omega(q) = 2^\alpha$ or $\omega(q) = 2^\alpha p$. Now, in light of Lemma 4, if $\omega(q) = 2^\alpha$ then $\lambda(q) = 2^{\alpha-1}$. Therefore, as $q \nmid V_{2^{\alpha-1}}(\sqrt{R}, Q)$, we have $\omega(q) = 2^\alpha p$ and $\lambda(q) = 2^{\alpha-1} p$. ∎

In an analogous manner, the following result is also established.

Theorem 2: *Let $q = 2^\alpha p + 1$, $\alpha \geq 1$, be any prime that satisfies either (6) or (7) and let $q \nmid RQ\Delta$. Then, $\omega(q) = 2^\alpha p$ and $\lambda(q) = 2^{\alpha-1}p$ if and only if $q \nmid V_{2^{\alpha-1}}(\sqrt{R}, Q)$.*

References

[1] R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Ann. of Math.*, 2nd Ser. **15** (1913): 30–70.

[2] D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.*, 2nd Ser. **31** (1930): 419–448.

[3] É. Lucas. "Théorie des Fonctions Numériques Simplement Périodiques." *Amer. J. Math.* **1** (1878): 184–240, 289–321.

[4] L. Somer. "Possible Periods of Primary Fibonacci-Like Sequences with Respect to a Fixed Odd Prime." *Fib. Quart.*, **20** (1981): 311–333.

Department of Mathematics & Physics,
Ave Maria University,
Ave Maria, FL 34142, U.S.A.
john.jaroma@avemaria.edu