Note on the Lucas–Lehmer Test

JOHN H. JAROMA

ABSTRACT. A proof of the Lucas–Lehmer test can be difficult to find, for most textbooks that state the result do not prove it. Over the past two decades, there have been some efforts to produce elementary versions of this famous result. However, the two that we acknowledge in this note did so by using either algebraic numbers or group theory. It also appears that in the process of trying to develop an elementary proof of this theorem, the original version provided by D. H. Lehmer's in 1930 has been overlooked. Furthermore, it is quite succinct and elementary, although by its style, it appears to have been written for an audience that has expertise in the theory of the extended Lucas sequences. Therefore, it is the primary objective of this paper to provide a brief introduction into the theory that underlies the said sequences, as well as to present an annotated version of Lehmer's original proof of the Lucas–Lehmer test. In conclusion, we show how the test may be utilized in order to identify certain composite terms of the Lucas numbers, $L_n = 1, 3, 4, 7, 11, 18, 29, \ldots$, with index equal to 2^n. A generalization to the companion Lehmer sequences is offered, as well.

1. Introduction

In 1878, E. Lucas proposed two tests in [6] for the primality of the Mersenne number, $N = 2^n - 1$. However, neither was accompanied by a complete proof. In 1930, and as part of his Ph.D. thesis, D. H. Lehmer stated and proved a necessary and sufficient condition for N to be prime [4]. This result has become known as the *Lucas–Lehmer test.* It is usually stated as follows.

2000 *Mathematics Subject Classification.* Primary 11A41; Secondary 11B39.
Key words and phrases. Prime, Fibonacci number, Lucas number, Lucas sequence, Lehmer sequence, Lucas–Lehmer test, Rank of apparition.

Theorem 1. *The number* $N = 2^n - 1$ *is prime if and only if* N *divides the* $(n-1)$*st term of the sequence*

$$4,\ 14,\ 194,\ 37634,\ \ldots,\ S_k,\ \ldots,$$

where $S_k = S_{k-1}^2 - 2$.

Demonstrations of Theorem 1 tend to be scarce, for most books that state the result do not prove it. In an interesting note that appeared in 1988, M. Rosen offered a demonstration of it using algebraic numbers [8]. In 1993, J. W. Bruce simplified part of Rosen's approach with group theory [1]. However, both arguments were given with the expressed intent of offering an elementary proof of Lehmer's result. Furthermore, [5] incorrectly cites [8] as the source containing Lehmer's original proof.

It is unfortunate that the first proof of Theorem 1 has not been widely disseminated, for it is succinct, elegant, and quite elementary. To be sure, some may encounter difficulty when initially trying to assimilate Lehmer's argument. The expository style presented in [4] tends to take for granted a knowledge of the theory of the extended Lucas sequences developed earlier in the paper, as well as omits supportive steps in the proof that may have been thought obvious to the initiated reader.

Therefore, it is our main objective to first introduce the requisite theory regarding the extended Lucas sequences, or Lehmer sequences, as they are known today and then utilize the results in order to produce a descriptive version of Lehmer's original proof of the Lucas–Lehmer test.

Our secondary objective is to show how the Lucas–Lehmer test may be interpreted in order to obtain an explicit condition for the compositeness of certain *Lucas numbers*, $L_n = 1, 3, 4, 7, 11, 18, 29, \ldots$, of index equal to a power of two. Unlike its counterpart, the *Fibonacci numbers* $F_n = 1, 1, 2, 3, 5, 8, \ldots$, where primes may occur only if the index of the underlying term is prime, a Lucas number is prime only if either its index is prime or equal to a power of two. The results shall then be extended to the companion Lehmer sequences.

We begin by defining the *rank of apparition* of a prime p to be the index of the first term in the underlying sequence that contains p as a divisor. Lehmer's argument relies materially on results introduced in [4] on the rank of apparition of a prime.

In the next section, we introduce the Lucas and Lehmer sequences. This will be followed by a description of some of the salient divisibility properties associated with the said recursive functions that we shall later utilize in our proof.

2. THE LUCAS SEQUENCES

Let P and Q be nonzero relatively prime integers. Then, the *Lucas sequences*, $\{U_n(P,Q)\}$, are defined by

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

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

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

Since (1) and (2) are linear, they are both solvable by identifying the roots of the characteristic equation,

$$X^2 - PX + Q = 0. \tag{3}$$

Let $D = P^2 - 4Q$ be the discriminant of (3). The roots of (3) may be described as

$$\alpha = \frac{P + \sqrt{D}}{2}, \qquad \beta = \frac{P - \sqrt{D}}{2}. \tag{4}$$

Using (4), we are now able to explicitly describe the Lucas sequences as

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n \in \{0, 1, \ldots\}. \tag{5}$$

In addition, the companion Lucas sequences are similarly given by

$$V_n(P,Q) = \alpha^n + \beta^n, \quad n \in \{0, 1, \ldots\}. \tag{6}$$

3. The Lehmer Sequences

In [4], Lehmer extended the theory of the Lucas sequences to similarly defined sequences where P is replaced by $\sqrt{R}$ and R is any integer relatively prime to Q. In the original theory of Lucas, the discriminant, $D = P^2 - 4Q$, cannot be of the form $4n+2$ or $4n+3$. This, in fact, motivated Lehmer's extension of the Lucas sequences.

The *Lehmer sequences*, $\{U_n(\sqrt{R}, Q)\}$, are recursively defined as

$$U_{n+2} = \sqrt{R}U_{n+1} - QU_n, \;\; U_0 = 0, \;\; U_1 = 1, \;\; n \in \{0, 1, \ldots\}. \tag{7}$$

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

$$V_{n+2} = \sqrt{R}V_{n+1} - QV_n, \;\; V_0 = 2, \;\; V_1 = \sqrt{R}, \;\; n \in \{0, 1, \ldots\}. \tag{8}$$

The characteristic equation of (7) and (8) is

$$X^2 - \sqrt{R}X + Q = 0. \tag{9}$$

Furthermore, the discriminant of (9) is

$$\Delta = R - 4Q. \tag{10}$$

Using (10), the roots of (9) are expressed as

$$\theta = \frac{\sqrt{R} + \sqrt{\Delta}}{2}, \qquad \phi = \frac{\sqrt{R} - \sqrt{\Delta}}{2}. \tag{11}$$

Thus, in light of (11), we have the following closed-end formula for the Lehmer sequences.

$$U_n(\sqrt{R}, Q) = \frac{\theta^n - \phi^n}{\theta - \phi}, \quad n \in \{0, 1, \ldots\}. \tag{12}$$

Similarly, the companion Lehmer sequences are also explicitly given by

$$V_n(\sqrt{R}, Q) = \theta^n + \phi^n, \quad n \in \{0, 1, \ldots\}. \tag{13}$$

4. Divisibility Properties of the Lehmer Sequences

Let p denote an arbitrary odd prime and assume that $p \nmid RQ$. The following lemmata are found in [4]. Each describes some characteristic property of the family of Lehmer sequences that will be needed in the proof of Theorem 1. We remark that the Lucas sequences are a subset of the Lehmer sequences. Thus, any theory presented in this section for the Lehmer and companion Lehmer sequences, necessarily applies also to the Lucas and companion Lucas sequences.

First, Lemma 1 tells us that no odd prime can be a factor of both a term of a Lehmer sequence, $U_n(\sqrt{R})\}$, and the corresponding term of the associated companion Lehmer sequence, $V_n(\sqrt{R}, Q)\}$.

Lemma 1. *The greatest common factor of $U_n(\sqrt{R}, Q)$ and of $V_n(\sqrt{R}, Q)$ is 1 or 2.*

We now introduce the following Legendre symbols:

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

The following lemma states that p necessarily divides either $U_{p-1}(\sqrt{R}, Q)$ or $U_{p+1}(\sqrt{R}, Q)$.

Lemma 2. $U_{p-\sigma\epsilon}(\sqrt{R}, Q) \equiv 0 \pmod{p}$.

Let $\omega(p)$ = *rank of apparition* of p in $\{U_n(\sqrt{R}, Q)\}$. Lemma 3 asserts that the only terms in a Lehmer sequence that contain p as a factor are those with index divisible by ω.

Lemma 3. *Let ω denote the rank of apparition of p in the sequence, $\{U_n(\sqrt{R}, Q)\}$. Then, $p \mid U_n(\sqrt{R}, Q)$ if and only if $n = k\omega$.*

The previous lemma may be illustrated, for example, by considering the prime $p = 23$ and the sequence $\{U_n(\sqrt{R}, Q)\} = \{U_n(1, -1)\}$. This Lehmer sequence produces the *Fibonacci numbers.* In it, the rank of apparition of p is 24 for $U_{24}(1, -1) = 46368 = 2^5 \cdot 3^2 \cdot 7 \cdot 23$ is the first term that contains 23 as divisor. Furthermore, we say that 23 is a *primitive factor* of $U_{24}(1, -1)$. Moreover, by Lemma 3, it follows that 23 divides infinitely many terms of $\{U_n(1, -1)\}$; specifically, all of those terms with index equal to $24k$, where k is any positive integer. Examples (with primitive factors underlined) include $U_{48}(1, -1) = 4807526976 = 2^6 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot \underline{1103}$, $U_{72}(1, -1) = 498454011879264 = 2^5 \cdot 3^3 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 107 \cdot \underline{103681}$, and $U_{96}(1, -1) = 51680708854858323072 = 2^7 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot \underline{769} \cdot 1103 \cdot 2207 \cdot \underline{3167}$.

The next lemma extends a result of R. D. Carmichael found in [2]. In particular, given the rank of apparition of p in $\{U_n(\sqrt{R}, Q)\}$, the parity of the index tells us whether or not p has a rank of apparition in the companion sequence, $\{V_n(\sqrt{R}, Q)\}$. In particular, if $\omega(p)$ is even, then p divides infinitely many identifiable terms of $\{V_n(\sqrt{R}, Q)\}$. Otherwise, no term of $\{V_n(\sqrt{R}, Q)\}$ may contain p as a factor.

Lemma 4. *Suppose that ω is odd. Then $V_n(\sqrt{R}, Q)$ is not divisible by p for any value of n. If n is even, say $2k$, then $V_{(2n+1)k}(\sqrt{R}, Q)$ is divisible by p for every n but no other terms of the sequence contain p as a factor.*

Recall that Lemma 2 gave us a sufficient condition for p to divide either $U_{p-1}(\sqrt{R}, Q)$ or $U_{p+1}(\sqrt{R}, Q)$. We may thus infer that the rank of apparition of any p such that $p \nmid RQ$ not only exists in $\{U_n(\sqrt{R}, Q)\}$ but also, it cannot be greater than $p \pm 1$. Unfortunately, Lemma 2 does not tell us if p divides any earlier term of the sequence. Nevertheless, the idea of Lemma 2 is extended in Lemma 5. It gives a necessary and sufficient condition for p to divide the earlier term, $U_{(p-\sigma\epsilon)/2}(\sqrt{R}, Q)$. The proof may be derived from work provided in [4] with a sketch of the idea presented in [7].

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

Finally, Lemma 6 is also found in [4]. It states an explicit condition in terms of rank of apparition for a number N to be prime. Moreover, it is a key tool used in Lehmer's original proof of Theorem 1.

Lemma 6. *If $N \pm 1$ is the rank of apparition of N then N is prime.*

5. Fundamental Identities

The following two identities will be needed.

$$U_{2n}(\sqrt{R}, Q) = U_n(\sqrt{R}, Q) \cdot V_n(\sqrt{R}, Q), \quad n \geq 0, \tag{14}$$

$$V_{2n}(\sqrt{R}, Q) = {V_n}^2(\sqrt{R}, Q) - 2Q^n, \quad n \geq 0. \tag{15}$$

6. Annotated Version of Lehmer's Proof

We are now ready to offer a descriptive version of Lehmer's original and elementary proof of Theorem 1.

Proof of Theorem 1. ($\Longrightarrow$) Assume that $N = 2^n - 1$ is prime. Consider the companion Lehmer sequence, $\{V_n(\sqrt{2}, -1)\}$.

Hence, $\Delta = R - 4Q = 6$.

Without loss of generality, we may assume that $n \geq 3$.[1] Thus, $N \equiv -1 \pmod 8$ and $\sigma = (R/N) = (2/N) = 1$. Furthermore, as $N \equiv -1 \pmod 4$, it follows by Gauss's Reciprocity Law that $(3/N) = (-N/3)$. Also, since

$$\epsilon = \left(\frac{\Delta}{N}\right) = \left(\frac{6}{N}\right) = \left(\frac{2}{N}\right)\left(\frac{3}{N}\right) = \left(\frac{3}{N}\right) = \left(\frac{-N}{3}\right) = -\left(\frac{N}{3}\right),$$

it follows that

$$\epsilon = -\left(\frac{N}{3}\right) \equiv -(2^n - 1)^{\frac{3-1}{2}} \equiv -\left[2\left(2^2\right)^{\frac{n-1}{2}} - 1\right] \equiv -1 \pmod 3.$$

In addition,

$$\tau = \left(\frac{Q}{N}\right) = \left(\frac{-1}{N}\right) = -1.$$

By Lemma 2, $N \mid U_{2^n}(\sqrt{2}, -1)$. However, by Lemma 5, $N \nmid U_{2^{n-1}}(\sqrt{2}, -1)$. Furthermore, by Lemma 3, $\omega(N) = 2^n$. Thus, because of Lemma 4, $N \mid V_{2^{n-1}}(\sqrt{2}, -1)$.

Finally, from (15),

$$V_{2^{k+1}}(\sqrt{2}, -1) = V_{2^k}^2(\sqrt{2}, -1) - 2(-1)^{2k}, \quad k \geq 0.$$

So, $V_2(\sqrt{2}, -1) = 4$, and for $k \geq 1$,

$$V_{2^{k+1}}(\sqrt{2}, -1) = V_{2^k}^2(\sqrt{2}, -1) - 2.$$

Hence, $S_k = V_{2^k}(\sqrt{2}, -1)$.

Therefore, $N \mid V_{2^{n-1}}(\sqrt{2}, -1)$; that is, $N \mid S_{n-1}$, the $(n-1)$st term of the sequence given in Theorem 1.

---

[1] If $n = 2$ then $N = 3$ is prime. However, $3 \nmid 4$. Thus, 3 does not divide the $(n-1)$st term of the sequence given in Theorem 1. Therefore, the Lucas–Lehmer test is not valid for $n < 3$. This restriction on n had not been explicitly noted by Lehmer in [4].

($\Longleftarrow$) Now, let us assume that $N \mid S_{n-1}$, where $S_k = S_{k-1}^2 - 2$ and $S_0 = 4$. Then,

$$N \mid V_{2^{n-1}}(\sqrt{2}, -1). \tag{16}$$

Because of (16) and (14), it follows that $N \mid U_{2^n}(\sqrt{2}, -1)$. However, by Lemma 1, $N \nmid V_{2^n}(\sqrt{2}, -1)$. Thus, because of Lemma 3, we have $\omega(N) = 2^r$, for some positive integer $r \leq n$. However, in light of (16) and Lemma 1, $N \nmid U_{2^{n-1}}(\sqrt{2}, -1)$. Applying Lemma 3 once more, we see that $\omega(N) = 2^n = N + 1$. Therefore, $N = 2^n - 1$ is prime, by Lemma 6. □

We point out that in view of (13), an alternative statement of the Lucas–Lehmer test is formulated as:

Theorem 2. (*Lucas–Lehmer*) *The number* $N = 2^n - 1$ *is prime if and only if* N *divides* $\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{2^{n-1}} + \left(\frac{\sqrt{2}-\sqrt{6}}{2}\right)^{2^{n-1}}$.

7. A Test for the Compositeness of L_{2^n}

The terms of the companion Lucas sequences given in (6) may be prime if n is either prime or a power of two. A similar conclusion holds for the companion Lehmer sequences given in (13). This result is known, but a proof can be difficult to find. Thus, we provide one here.

Lemma 7. *Let* $\{V_n(\sqrt{R}, Q)\}$ *be a companion Lehmer sequence. If* $V_n(\sqrt{R}, Q)$ *is prime, then either* n *is prime or* $n = 2^k$, *for* $k \geq 1$.

Proof. Let V_n, $n > 2$, be a term of a companion Lehmer sequence in which n is neither prime nor a power of two. Then, $n = mq$, where $m \geq 2$ and p is an odd prime. Now, V_m contains at least one prime factor, say π. Thus, by Lemma 4, $\pi \mid V_{mp}$. Furthermore, this means that π is a nonprimitive prime factor of V_n. Therefore, V_n must be composite. □

An open question is whether or not the Lucas numbers, $\{L_n\} = \{V_n(1, -1)\}$, (the companion sequence to the Fibonacci numbers) contain infinitely many primes. Recently, H. Dubner and W. Keller announced that L_{14449} is prime and provided a list of known, as well as probable Lucas primes with indices $n \leq 50,000$ [3]. Although no such prime was given with index $2^k > 16$, we do not know if L_{16} is the largest such Lucas prime.

We now wish to point out that the Lucas–Lehmer test may be restated in order to provide a necessary and sufficient condition for certain L_{2^k} to be composite. In particular, recall that in the proof of Theorem 1, if $N \mid S_{n-1}$ then $N \mid V_{2^{n-1}}(\sqrt{R}, Q)$. In such instances, not only is N prime but as long as $N < V_{2^{n-1}}$, then $V_{2^{n-1}}$ is necessarily composite. Thus, in order that we may establish for certain Mersenne primes, N, that $N \mid L_{2^{n-1}}$, it remains for us to find a set of conditions under which the counterpart Fibonacci sequence, $\{U_n(1,-1)\}$, may replace $\{U_n(\sqrt{2},-1)\}$ in the proof of Theorem 1.

To this end, since $\sqrt{R} = 1$ and $Q = -1$, it follows that $R = 1$ and $\Delta = 5$. Hence, if $n \equiv 3 \pmod 4$, then $\epsilon = (\Delta/N) = -1$. Furthermore, $\sigma = (R/N) = (1/N) = 1$ and as long as $n \geq 2$, then $\tau = (Q/N) = (-1/N) = -1$. Finally, if $n > 3$ then $N < L_{2^{n-1}}$. Thus, since N can be prime only if n is prime, we have the following theorem and corollary.

Theorem 3. *Let $N = 2^p - 1$, where p is any prime satisfying $p \equiv 3 \pmod 4$. Then, $N \mid \left[\left(\frac{1+\sqrt{5}}{2}\right)^{2^{p-1}} + \left(\frac{1-\sqrt{5}}{2}\right)^{2^{p-1}}\right]$ if and only if N is prime.*

Corollary 1. *Let $N = 2^p - 1$, where $p \equiv 3 \pmod 4$ is prime. Then, $L_{2^{p-1}}$ is composite.*

8. A Test for the Compositeness of $V_{2^n}(\sqrt{R}, Q)$

As just observed, the use of the sequence, $\{U_n(\sqrt{2},-1)\}$, in Lehmer's proof is not required provided that we can find an alternative sequence, $\{U_n(\sqrt{R},Q)\}$, where $\epsilon = -1$ and $\sigma \cdot \tau = -1$. In [4], Lehmer demonstrates that either the sequence $\{U_n(98,-1)\}$ or the sequence $\{U_n(14,-1)\}$ may be used with every $2^n - 1$ as long as n is odd. Thus, given such a sequence, as well as a $\kappa > 0$ for which $n > \kappa$ implies that $N < |V_n(\sqrt{R},Q)|$, we state the following theorem and corollary.

Theorem 4. *Let $\{U_n(\sqrt{R},Q)\}$ be a Lehmer sequence satisfying both $\epsilon = -1$ and $\sigma \cdot \tau = -1$. Then $N = 2^n - 1$ is prime if and only if $N \mid \left[\left(\frac{\sqrt{R}+\sqrt{\Delta}}{2}\right)^{2^{n-1}} + \left(\frac{\sqrt{R}-\sqrt{\Delta}}{2}\right)^{2^{n-1}}\right]$.*

Corollary 2. *Let $\{V_n(\sqrt{R}, Q)\}$ be a companion Lehmer sequence satisfying $\epsilon = -1$ and $\sigma \cdot \tau = -1$. Also let $N = 2^n - 1$ be prime and $\kappa > 0$ be any positive integer such that $n > \kappa$ implies that $N = 2^n - 1 < |V_{2^n-1}(R, Q)|$. Then, $V_{2^n-1}(\sqrt{R}, Q)$ is composite.*

REFERENCES

[1] J. W. Bruce, *A really trivial proof of the Lucas–Lehmer test*, Amer. Math. Monthly, **100** (1993), 370–371.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Annals of Mathematics, 2nd Ser., **15** (1913), 30–70.

[3] H. Dubner, W. Keller, *New Fibonacci and Lucas primes*, Mathematics of Computation, **68** (1999), 417–427.

[4] D. H. Lehmer, *An extended theory of Lucas' functions*, Annals of Mathematics, 2nd Ser., **31** (1930), 419–448.

[5] D. H. Lehmer, *On Lucas' test for the primality of Mersenne's numbers*, J. of the London Math. Soc., **10** (1935) 162–165.

[6] É. Lucas, *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics, **1** (1878), 184–240, 289–321.

[7] P. Ribenboim, *The New Book of Prime Number Records*, New York: Springer-Verlag, 1996.

[8] M. Rosen, *A proof of the Lucas–Lehmer test*, Amer. Math. Monthly, **95** (1988), 855–856.

John H. Jaroma,
Department of Mathematics & Computer Science,
Austin College,
Sherman, TX 75090 U.S.A.,
jjaroma@austincollege.edu

Received on 25 October 2004.