EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 2, No. 3, 2009, (352-360)
ISSN 1307-5543 – www.ejpam.com

Equivalence of Pepin's and the Lucas-Lehmer Tests

John H. Jaroma

Department of Mathematics & Physics, Ave Maria University, Ave Maria, Florida, 34142, UNITED STATES

Abstract. Pepin's test provides a necessary and sufficient condition for a Fermat number to be prime. The Lucas-Lehmer test does similarly for a Mersenne number. These tests share a common nature. However, this is evident neither by their usual statements nor their usual treatment in the literature. Furthermore, it is unusual to even find a proof of the latter result in elementary textbooks. The intent of this paper is to bring to light the equivalent structure of these two primality tests.

2000 Mathematics Subject Classifications: 11A41, 11A51, 11B39

Key Words and Phrases: Primes, primality test, Lehmer sequence, Pepin's test, Lucas-Lehmer test.

1. Introduction

A *Fermat number* is any integer of the form $F_n = 2^{2^n} + 1$, where $n \geq 0$. They are named in honor of Pierre de Fermat (1601–1665) who had expressed a belief that such numbers are always prime. In 1732, Leonhard Euler negatively resolved

Fermat's assertion by factoring F_5. Today, the prevailing conjecture appears to be that no Fermat primes beyond $n = 4$ exist. A necessary and sufficient condition for the primality of a Fermat number is provided by *Pepin's test*. It is named after Fr. Théophile Pepin (1826–1904) and is found in textbooks often stated along the lines of F_n *is prime if and only if* $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ [1], [11], or [15].

A *Mersenne number* is any integer given by $M_n = 2^n - 1$, where $n \geq 1$, and so called because of a rather accurate conjecture made by Fr. Marin Mersenne (1588–1648) who asserted that such numbers are prime for $n \in \{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$ and composite for all other values of $n \leq 257$. It took mathematicians more than 300 years to completely resolve the conjecture. Upon having done so, we learned that Mersenne had made only five mistakes. The *Lucas-Lehmer test* provides a necessary and sufficient condition for a Mersenne number to be prime. Letting p denote a prime, the test is often described as M_p *is prime if and only if* $r_{p-1} \equiv 0 \pmod{M_p}$, *where* $r_1 = 4$, *and for* $k \geq 2$, $r_k = r_{k-1}^2 - 2 \pmod{M_p}$, $0 \leq r_k < M_p$. For instance [1], [13] or [14].

Although not evident by their usual statements alone, both Pepin's test and the Lucas-Lehmer test are inherently derived from the properties of the Lehmer sequences with both tests being demonstrable by similar arguments. The intent of this note to make the common structure of these two tests more widely known.

The similarity between the two primality tests appears to have been overlooked. For example, in [10], Pepin's test is discussed after the section *Primality tests based on the Lucas sequences*.* In addition, in [3], Derrick Lehmer opts not to illustrate a test for the primality of the Fermat numbers but instead remarks *in particular we could give new tests for the primality of* $2^{2^n} + 1$, *but those Fermat numbers which have not already been tested are too large for the application of any known test.* Having said this, Pepin's test is never explicitly mentioned in Lehmer's paper. Lastly, in [16], Williams

*The Lucas sequences are special cases of the Lehmer sequences, where R is a perfect square.

cites that Pepin had been aware that the earlier version of his test, $N = 2^r + 1$ *is prime if and only if* $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$, could be made into a simple Lucas-like test by defining $T_1 = 5^2$ and $T_{i+1} = T_i^2$, where i is a positive integer. This leads to the result that F_n is prime if and only if $F_n \mid T_{r-1} + 1$. However, a direct correlation to the Lucas-Lehmer result does not appear to be given in the book.

2. The Lehmer Sequences

Let R and Q be relatively prime integers. The *Lehmer sequences* $\{U_n(\sqrt{R}, Q)\}$ and the *companion Lehmer sequences* $\{V_n(\sqrt{R}, Q)\}$ are defined respectively, by

$$U_{n+2}(\sqrt{R}, Q) = \sqrt{R}U_{n+1} - QU_n, \;\; U_0 = 0, \;\; U_1 = 1, \;\; n \in \{0, 1, \ldots\} \tag{2.1}$$

$$V_{n+2}(\sqrt{R}, Q) = \sqrt{R}V_{n+1} - QV_n, \;\; V_0 = 2, \;\; V_1 = \sqrt{R}, \;\; n \in \{0, 1, \ldots\}. \tag{2.2}$$

Furthermore, since (2.1) and (2.2) are linear, they are solvable and given explicitly by (2.3) and (2.4), respectively.

$$U_n(\sqrt{R}, Q) = \frac{\theta^n - \phi^n}{\theta - \phi}, \quad n \in \{0, 1, \ldots\} \tag{2.3}$$

$$V_n(\sqrt{R}, Q) = \theta^n + \phi^n, \quad n \in \{0, 1, \ldots\} \tag{2.4}$$

where, $\theta = \frac{\sqrt{R} + \sqrt{R - 4Q}}{2}$ and $\phi = \frac{\sqrt{R} - \sqrt{R - 4Q}}{2}$.

We say that the *rank of apparition* of a number N in a sequence is the index of the first term in that sequence that contains N as a divisor. N is said to have *maximal* rank of apparition provided that its rank of apparition is either $N \pm 1$.

3. Properties of the Lehmer Sequences

Let p denote an arbitrary odd prime such that $p \nmid RQ$. The following propositions are divisibility properties associated with the Lehmer sequences found in [3].

Lemma 3.1. *The greatest common factor of $U_n(\sqrt{R},Q)$ and $V_n(\sqrt{R},Q)$ is 1 or 2.*

Let p be an odd prime and a any integer not divisible by p. Then, the *Legendre symbol* (a/p) is defined to be 1 provided that a is a quadratic residue modulo p and -1 if a is a quadratic nonresidue modulo p. For all a such that $(a,p)=1$, a is called a *quadratic residue modulo p* if the congruence $x^2 \equiv a \pmod{p}$ has a solution. Otherwise, a is called a *quadratic nonresidue modulo p*. If $p \mid a$ then $(a/p)=0$. Consider the Legendre symbols $\sigma=(R/p)$ and $\epsilon=(\Delta/p)$, where $\Delta=R-4Q$ is the discriminant of the characteristic equation of (2.1) and (2.2).

Lemma 3.2. *Let $p \nmid RQ$. Then, $U_{p-\sigma\epsilon}(\sqrt{R},Q) \equiv 0 \pmod{p}$.*

Let $\omega(p)$ denote the rank of apparition of p in $\{U_n(\sqrt{R},Q)\}$. The next result tells us that every term with index equal to a multiple of ω must also contain p as a factor.

Lemma 3.3. *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 $n=k\omega$, where $k \in \{1,2,\ldots\}$.*

So far, we have seen that almost any odd prime will divide infinitely many terms of $\{U_n(\sqrt{R},Q)\}$. However, there are infinitely many p which do not divide $\{V_n(\sqrt{R},Q)\}$.

Lemma 3.4. *Suppose that ω is odd. Then $V_n(\sqrt{R},Q)$ is not divisible by p for any value of n. On the other hand, 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.*

Let $\lambda(p)$ denote the rank of apparition of p in $\{V_n(\sqrt{R},Q)\}$.

Lemma 3.5. *Let $p \nmid RQ\Delta$. Then, $U_{\frac{p-\sigma\epsilon}{2}}(\sqrt{R},Q) \equiv 0 \pmod{p}$ if and only if $\sigma=\tau$, where $\tau=(Q/p)$.*

Lemma 3.6. *Let $p \nmid 2RQ\Delta$. If $N \pm 1$ is the rank of apparition of N then N is prime.*

4. Historical Background

In order to acquire a more complete understanding of these two tests, we consider them first in their historical contexts. In 1877, Fr. Pepin formulated the following theorem [7]:

Theorem 4.1. *Pepin's Test (Original Version)* The Fermat number, $F_n = 2^{2^n} + 1$, where $n > 1$ is prime if and only if

$$5^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Pepin had noted in [7] that the number 10 could be used in place of 5. Prior to Pepin's remark, François Proth (1852 – 1879) noted in 1876 and then again in 1878 that one may use the number 3 in lieu of 5 for our Theorem 4.1 [8], [9]) but offered no proof of his assertion. Then, Édouard Lucas (1842 – 1891) commented that an arbitrary integer a could be used in place of 5 provided that the Jacobi symbol (a/F_n) has a value equal to -1 [5] and in 1879 offered a proof [6]. Thus, the result we now call *Pepin's test* is actually a theorem suggested by Proth and proved by Lucas. For a more detailed summary of these events, the reader is directed to [16], where a more detailed account is found. A modern version of Pepin's test is given by:

Theorem 4.2. *Pepin's Test (Modern Version)* The Fermat number, $F_n = 2^{2^n} + 1$, where $n \geq 1$ is prime if and only if

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Testing primality of the Mersenne numbers was initiated by Lucas in 1878. Lucas proposed two tests for determining if $2^n - 1$ is prime [5]. However, neither theorem

was given as necessary and sufficient. In 1930, D. H. Lehmer wrote, *his [Lucas's] conditions for primality are sufficient but not necessary.*[†] *One is uncertain whether Lucas' tests will reveal the character of a number which is actually a prime* [3]. Lehmer furthermore noted that R. D. Carmichael in [2] had provided a set of necessary and sufficient conditions for the primality of such numbers. However, with the exception of two cases, they depended on the existence of an auxiliary pair of numbers to be used in testing a given integer. Thus, according to Lehmer, *from a practical point of view these tests are not applicable since no method is given for determining in advance an appropriate number pair.* Finally, in response to his own observation Lehmer produced an explicit necessary and sufficient condition for a Mersenne number to be prime [3]. This result today is commonly known as the *Lucas-Lehmer test*.

The original statement of this celebrated result is found in [3], although it had been mistakenly noted in [13] that Lehmer's original proof of the Lucas-Lehmer test is given in [4].

Theorem 4.3. *Lucas-Lehmer Test (Original Version)* The number, $M_n = 2^n - 1$, is prime if and only if it divides the $(n-1)st$ term of the sequence

$$4,\ 14,\ 194,\ 37634,\ 1416317954,\ \ldots\ S_k,\ \ldots\ where,\ S_k = S^2{}_{k-1} - 2.$$

5. Equivalence of Pepin's and the Lucas-Lehmer Tests

We are ready to show that Pepin's and the Lucas-Lehmer tests share a similar structure. To this end, we make the observation that $\{V_n(4,3)\} = 3^n + 1$. This follows subsequently from Theorem 5.1.

[†]*Although Lucas did not attempt to give necessary tests, one of them is in fact necessary.*

Theorem 5.1. *Let a be any integer. Then the terms of the companion Lehmer sequence $\{V_n(\sqrt{R},Q)\} = \{V_n(a+1,a)\}$ are of the form a^n+1.*

The proof is straightforward in light of (2.4) by letting $\sqrt{R} = a+1$ and $Q = a$, and is omitted. Hence, the terms of $\{V_n(4,3)\}$ are $V_n = 3^n+1$. So, $V_{\frac{F_n-1}{2}} = 3^{\frac{F_n-1}{2}}$. Thus, Theorem 4.2 is revised equivalently by the statement of Theorem 5.2. Its proof requires the following identity found in [3].

$$U_{2n} = U_n V_n \tag{5.1}$$

Theorem 5.2. *Pepin's Test* The Fermat number $F_n = 2^{2^n}+1$ where, $n \geq 1$ is prime if and only if

$$F_n \mid V_{\frac{F_n-1}{2}}(4,3).$$

Proof. Consider $\{V_n(4,3)\}$. Then, $\Delta = R-4Q = 16-12 = 4$. Letting $F_n = 2^{2^n}+1$ be prime, it follows that $\epsilon = \left(\frac{\Delta}{F_n}\right) = \left(\frac{4}{F_n}\right) = \left(\frac{2}{F_n}\right)\left(\frac{2}{F_n}\right) = 1$ and $\sigma = \left(\frac{R}{F_n}\right) = \left(\frac{16}{F_n}\right) = \left(\frac{4}{F_n}\right)\left(\frac{4}{F_n}\right) = 1$. Furthermore, since $n > 1$, by Gauss's Reciprocity Law, $\left(\frac{3}{F_n}\right)\left(\frac{F_n}{3}\right) = \left(\frac{3}{2^{2^n}+1}\right)\left(\frac{2^{2^n}+1}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{2^{2^n}+1-1}{2}} = (-1)^{2^{n-1}} = 1$. Hence, $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$. Thus, $\tau = \left(\frac{Q}{F_n}\right) = \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) \equiv \left(2^{2^n}+1\right)^{\frac{3-1}{2}} \equiv -1 \pmod 3$. Since $\sigma\epsilon = 1$, then by Lemma 3.2, $F_n \mid U_{2^{2^n}}$. Because $\tau \neq \sigma$, it follows by Lemma 3.5 that $F_n \nmid U_{2^{2^n-1}}$. Thus, the rank of apparition of F_n in $\{U_n(4,3)\}$ is 2^{2^n}; that is, $F_n - 1$. (Otherwise, by Lemma 3.3 the rank of apparition is 2^{2^n-r}, for some positive integer r. Also by Lemma 3.3, $F_n \mid U_{2^{n-1}}$.) Therefore, by Lemma 3.4, $F_n \mid V_{\frac{F_n-1}{2}}$. Conversely, let's suppose $F_n \mid V_{\frac{F_n-1}{2}}$. Then by (5.1), $F_n \mid U_{F_n-1}$. Specifically, $F_n \mid U_{2^{2^n}}$. By Lemma 3.3, $\omega(F_n)$ must be a divisor of 2^{2^n}. But by Lemma 3.1, $U_{2^{2^n}}$ is relatively prime to $U_{2^{2^n-1}}$. Thus, $\omega(F_n) = 2^{2^n} = F_n - 1$. Therefore, by Lemma 3.6, F_n is prime.

Next, we show that the sequence of numbers 4, 14, 194, 37634, 1416317954, ... given in Theorem 4.3 are the terms of the companion Lehmer sequence $\{V_n(\sqrt{2},-1)\}$

whose indices are powers of 2. But first, the following identity found in [3] is needed.

$$V_{2n} = V_n^2 - 2Q^n. \tag{5.2}$$

Now, consider $\{V_n(\sqrt{2}, -1)\}$. So, $V_2 = 4$. Furthermore, from Theorem 4.3 $S_k = S_{k-1}^2 - 2$, where $S_1 = 4 = V_2$. Since $Q = -1$, by (5.2) it follows that $S_k = V_{2^k}$ for $k \in \{1, 2, \ldots\}$. Hence, the statement given in the Lucas-Lehmer Test asserting M_n *divides the* $(n-1)st$ *term of 4, 14, 194, 37634, 1416317954,* ... then M_n *is a factor of* $V_{2^{n-1}}$ is equivalent to saying that $M_n \mid V_{\frac{M_n+1}{2}}$. Thus, we now state the following equivalent form of Theorem 4.3.

Theorem 5.3. *Lucas-Lehmer Test* The number $M_n = 2^n - 1$, where $n > 2$ is prime if and only if

$$M_n \mid V_{\frac{M_n+1}{2}}(\sqrt{2}, -1).$$

Proof. As $R = 2$, $Q = -1$, and $\Delta = 6$, it follows that $\epsilon = -1$, $\sigma = 1$, and $\tau = -1$. The proof then follows similarly to that presented for Theorem 5.2. It may be found in [3].

References

[1] D. M. Burton, *Elementary Number Theory*, 6th ed., McGraw-Hill, New York, 2005.

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

[3] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. Math.* 31: 419–448 (1930).

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

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

[6] É. Lucas, Question 453, *Nouv. Cor. Math.* 5: p.137 (1879).

[7] T. Pepin, Sur la formule $2^{2^n}+1$, *Comp. Rend. Acad. Sci.* 85: 329–331 (1877).

[8] F. Proth, Énoncés de divers théorèmes sur les nombres, *Comp. Rend. Acad. Sci.* 83: 1288–1289 (1876).

[9] F. Proth, Mémoires présentés, *Comp. Rend. Acad. Sci.* 87: p.374 (1878).

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

[11] N. Robbins, *Beginning Number Theory*, Wm. C. Brown, Dubuque, 1993.

[12] K. H. Rosen, *Elementary Number Theory*, 4th ed., Addison Wesley Longman, Reading, 2000.

[13] M. Rosen, A proof of the Lucas-Lehmer test, *Amer. Math. Mon.* 95: 855–856 (1988).

[14] P. Schumer, *Introduction to Number Theory*, PWS, Boston, 1996.

[15] J. J. Tattersall, *Elementary Number Theory in Nine Chapters*, 2nd ed., Cambridge Univ. Press, Cambridge, 2005.

[16] H. C. Williams, *Édouard Lucas and Primality Testing*, John Wiley & Sons, New York, 1998.