A NOTE ON PRIMALITY TESTS FOR $N = h \cdot 2^n - 1$

ÖYSTEIN J. RÖDSETH

Department of Mathematics, University of Bergen,

Allégt. 55, N-5007 Bergen, Norway

rodseth@mi.uib.no

Abstract

Using only the most simple properties of the finite field $\mathbf{F}_{p^2}$, we give a short proof of Riesel's primality test for integers of the form $N = h \cdot 2^n - 1$.

AMS Subject Classification: 11A51, 11Y11.

Lucas [10] gave two tests which show whether $2^n - 1$, n odd, is prime or not. But he never published any proof of either. The "first" test is valid only if $n \equiv 3 \pmod 4$, while the "second" test is valid for any odd n. Therefore the second test is the most interesting. In 1930, Lehmer [8] gave an "arithmetical" proof of the second test. In 1932, Western [16] gave "algebraic" proofs of both tests, and also of that of Pepin [11], first proved by Carmichael [4].

However, as late as in 1988, Rosen [14] is not completely satisfied with the situation. He says that: " ... it is hard to find a proof (of the second test) in a modern text. Most books which state the result do not prove it, but do prove a related and weaker result (the first test), e.g. [5], [6]. In [15] a complete proof is given which follows the original proof of D. H. Lehmer (see [9]), but it is lengthy and detailed."

The algebraic proofs of the two tests are much shorter than the arithmetical ones. And the algebraic proof of the first test is simpler than that of the second test. The algebraic proofs use properties of algebraic numbers. For the proof of the first test, Western uses the field $K = \mathbf{Q}(\sqrt{5})$, and for the proof of the second test, Western uses the field $K = \mathbf{Q}(\sqrt{3})$, as suggested to him by D. H. Lehmer. The latter field is also used by Rosen [14] in his more recent variant of Western's proof of the second test. In these proofs one works in the ring $\mathcal{O}_K$ of algebraic integers $a + b\omega$, $a, b \in \mathbf{Z}$, where $\omega = (1 + \sqrt{5})/2$ if $K = \mathbf{Q}(\sqrt{5})$, and $\omega = \sqrt{3}$ if $K = \mathbf{Q}(\sqrt{3})$. One considers various algebraic integers $a + b\omega$ (or rather a and b) modulo π, where π is a prime in $\mathcal{O}_K$. However, both Western and Rosen

overlook the fact that it is not necessary to consider non-rational primes in $\mathcal{O}_K$. Thus we are looking at $a + b\omega$, where a and b are considered modulo a rational prime p that doesn't split in $\mathcal{O}_K$. This indicates that the proper environment for algebraic proofs of the Lucas-tests is the finite field $\mathbf{F}_{p^2}$. And in 1951, Brewer [1] gave a short proof of the second Lucas test (the Lucas-Lehmer test) using the finite field $\mathbf{F}_{p^2}$. However, Brewer's proof of the Lucas-Lehmer test does not seem to have received the attention it deserves. A possible reason for this is that there are some gaps in the proofs of some of the other theorems in Brewer's paper; cf. de Bruijn [3].—Recently Bruce [2] gave a proof of the sufficiency of the test. His proof has much in common with that of Brewer. Even though Bruce actually works in (the multiplicative group of) the field $\mathbf{F}_{p^2}$, he carefully avoids the notion of a finite field, and uses only terminology from group theory.

Lucas' two tests and Pepin's test are special cases of the theorem of Riesel [12, Theorem 5], [13, Theorem 4.17]. Also Riesel proved his result by using properties of quadratic fields, but unlike some of the authors mentioned above, Riesel knew that it is not necessary to consider non-rational primes.—In this note we present an alternative proof of a simplified, but equivalent, version of Riesel's theorem, using only the most simple properties of the field $\mathbf{F}_{p^2}$. However, in the theorem below we replace Riesel's condition $h < 2^n$ by the weaker condition $h < 2^{n+1} - 1$. By excluding certain composite values of N, the bound $2^{n+1} - 1$ can also be replaced by larger bounds; cf. Inkeri [7, p. 7].

For various initial integer values of S_1, we shall consider an integer sequence $S_1, S_2, \ldots$ satisfying the recurrence relation

$$S_{i+1} = S_i^2 - 2 \quad \text{for } \ i \geq 1.$$

In the theorem below, P is a rational integer, and the statement involves the term V_h of the Lucas sequence $\{V_i\}$ given by

$$V_0 = 2, \quad V_1 = P, \quad V_{i+1} = PV_i - V_{i-1} \ \ (i \geq 1).$$

The term V_h can quickly be computed by the formulas

$$V_{2i} = V_i^2 - 2, \quad V_{2i+1} = V_i V_{i+1} - P.$$

Also, the Legendre-Jacobi symbol is denoted by (/).

THEOREM. *Let n, h be integers, where $n > 1$, h is odd, and $0 < h < 2^{n+1} - 1$. Put $N = h \cdot 2^n - 1$ and let $S_1 = V_h$ for some integer P satisfying*

$$\left(\frac{P-2}{N}\right) = 1, \quad \left(\frac{P+2}{N}\right) = -1. \tag{1}$$

Then N is a prime if and only if $S_{n-1} \equiv 0 \pmod{N}$.

PROOF. Put $D = (P-2)(P+2)$. Then $(D/N) = -1$, and there is a prime divisor p of N satisfying $(D/p) = -1$.

Let $\sigma \in \mathbf{F}_{p^2}$ satisfy $\sigma^2 = D$. (The existence of σ is trivial from the representation of $\mathbf{F}_{p^2}$ as $\mathbf{F}_p[x]/(x^2 - D)$.) Further, put $\alpha = (P+2+\sigma)^2/4(P+2)$. Then $\alpha^{-1} = (P+2-\sigma)^2/4(P+2)$, and by considering $\{S_i\}$ as a sequence in (the prime field of) $\mathbf{F}_{p^2}$, we have $V_i = \alpha^i + \alpha^{-i}$, $S_i = \alpha^{h \cdot 2^{i-1}} + \alpha^{-h \cdot 2^{i-1}}$.

By the binomial theorem, Fermat's little theorem, and Euler's criterion, we have $(P+2+\sigma)^p = P+2-\sigma$, and it follows that

$$\alpha^{(p+1)/2} = \left(\frac{P+2}{p}\right). \tag{2}$$

Now, suppose that $S_{n-1} \equiv 0 \pmod{N}$. Then $S_{n-1} = 0$ in $\mathbf{F}_{p^2}$, so that $\alpha^{h \cdot 2^{n-1}} + 1 = \alpha^{h \cdot 2^{n-2}} S_{n-1} = 0$. Hence 2^n divides the multiplicative order of α in $\mathbf{F}_{p^2}^*$. By (2), $\alpha^{p+1} = 1$, so that $p + 1 = 2^n k$ for some integer $k \geq 1$. Hence $h \cdot 2^n - 1 = N = (2^n k - 1)q$, and it is easily seen that $q = 2^n m + 1$ for some integer m. Suppose that $N \neq p$. Then $m \geq 1$. If $k = m = 1$, then $h = 2^n$, contradicting the fact that h is odd. Hence $k \geq 2$ or $m \geq 2$, and it follows that $h \geq 2^{n+1} - 1$.

On the other hand suppose that $N = p$. By (1) and (2), we then have $\alpha^{(p+1)/2} = -1$, and multiplication by $\alpha^{-(p+1)/4}$ gives $S_{n-1} = 0$, that is $S_{n-1} \equiv 0 \pmod{N}$, and the proof of the theorem is complete.

Also if (1) does not hold, we have that $S_{n-1} \equiv 0 \pmod{N} \Rightarrow N$ prime. It is, however, an easy exercise to convince oneself of that (1) is the only case of interest.

Putting $P = 4$, we find by reciprocity that (1) holds if $n \geq 3$ and

$$h \equiv (-1)^{n-1} \pmod{3}. \tag{3}$$

Hence we have the following corollary, cf. [13, Theorem 4.16].

COROLLARY 1. *Let $n \geq 3$, h odd, $0 < h < 2^{n+1} - 1$. Suppose that (3) holds, and put $P = 4$. Then $N = h \cdot 2^n - 1$ is a prime if and only if $S_{n-1} \equiv 0 \pmod{N}$.*

Note that if $h \equiv (-1)^n \pmod{3}$, then N is divisible by 3.

In particular, for $h = 1$ and n odd, Corollary 1 gives us the celebrated Lucas-Lehmer Test.

COROLLARY 2 (Lucas-Lehmer). *Let $n > 1$ be odd, and put $S_1 = 4$. Then $N = 2^n - 1$ is a prime if and only if $S_{n-1} \equiv 0 \pmod{N}$.*

Although this result holds for any odd $n > 1$, the test would, of course, be used only if n is a prime.

Putting $P = 3$, $h = 1$, and assuming $n \equiv 3 \pmod 4$, the theorem gives us Lucas' first test.

Finally, let $h = 1$, and let b, c be integers such that $\gcd(b^2 + c^2, N) = 1$. Putting $P \equiv 2(b^2 - c^2)/(b^2 + c^2) \pmod N$, the theorem gives us Pepin's test. (Pepin also assumes that $b^2 + c^2$ is a prime.)

References

[1] Brewer, B. W., *Tests for primality*, Duke Math. J. 18, 757–763 (1951).

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

[3] de Bruijn, N. G., Math. Rev. 13, 208 (1952).

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

[5] Hardy, G. H., Wright, E. M., *An Introduction to the Theory of Numbers*, Fourth ed., Clarendon Press, Oxford 1968.

[6] Hua, L. K., *Introduction to the Theory of Numbers*, Springer-Verlag, Berlin 1982.

[7] Inkeri, K., *Tests for primality*, Ann. Acad. Sci. Fenn. A I 279, 1–19 (1960). Reprinted in *Collected Papers of Kustaa Inkeri* (Metsänkylä, T., Ribenboim, P., eds.), Queen's Papers in Pure and Applied Mathematics, Vol. 91, 327–345, Kingston 1992.

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

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

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

[11] Pepin, T., *Sur la formule* $2^n - 1$, C. R. Acad. Sci. Paris 86, 307–310 (1878).

[12] Riesel, H., *Lucasian Criteria for the Primality of* $N = h \cdot 2^n - 1$, Math. Comp. 23, 869–875 (1969).

[13] Riesel, H., *Prime Numbers and Computer Methods for Factorization*, Birkhauser, Boston 1985.

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

[15] Sierpinski, W., *Elementary Theory of Numbers*, Polski Akademic Mauk., Warsaw 1964.

[16] Western, A. E., *On Lucas' and Pepin's tests for the primeness of Mersenne numbers*, J. London Math. Soc. 7, 130–137 (1932).