A Proof of the Lucas-Lehmer Test

MICHAEL I. ROSEN*
Department of Mathematics, Brown University, Providence, Rhode Island 02912

E. Lucas proposed and D. H. Lehmer proved a very elegant test for the primality of the Mersenne number $M_p = 2^p - 1$. Unfortunately, it is hard to find a proof in a modern text. Most books which state the result do not prove it, but do prove a related and weaker result, e.g. [**1**], [**2**], and [**4**]. In [**5**] a complete proof is given which follows the original proof of D. H. Lehmer (see [**3**]), but it is lengthy and detailed. In this note I give a fairly short proof using the simplest properties of algebraic numbers. Another proof using algebraic numbers was given long ago in [**6**].

Define a sequence S_n recursively by setting $S_1 = 4$ and $S_n = S_{n-1}^2 - 2$. So, $S_1 = 4$, $S_2 = 14$, $S_3 = 194$, etc.

THEOREM (LUCAS-LEHMER). *Let p be a prime number. Then, $M_p = 2^p - 1$ is a prime if and only if M_p divides S_{p-1}.*

Before giving the proof we need a few definitions. Let

$$\tau = \frac{1 + \sqrt{3}}{\sqrt{2}}, \quad \bar{\tau} = \frac{1 - \sqrt{3}}{\sqrt{2}}, \quad \omega = \tau^2 = 2 + \sqrt{3}, \quad \text{and } \bar{\omega} = \bar{\tau}^2 = 2 - \sqrt{3}.$$

Note that $\tau\bar{\tau} = -1$ and $\omega\bar{\omega} = 1$.

LEMMA. $S_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$.

Proof. Let $T_m = \omega^{2^{m-1}} + \bar{\omega}^{2^{m-1}}$. Then $T_1 = \omega + \bar{\omega} = 4 = S_1$ and $T_{m+1} = T_m^2 - 2$. Thus, $T_m = S_m$ for all m.

LEMMA 2. *If we assume M_p is prime, then $\tau^{M_p+1} \equiv -1 \pmod{M_p}$.*

Proof. The congruence is understood to take place in the ring of algebraic integers. We temporarily set $q = M_p$.

Write $\sqrt{2}\,\tau = 1 + \sqrt{3}$, raise both sides to the qth power and take congruences modulo q. We find

$$\tau^q 2^{(q-1)/2}\sqrt{2} \equiv 1 + 3^{(q-1)/2}\sqrt{3} \pmod{q}.$$

Since $q \equiv -1 \pmod 8$ we have $2^{(q-1)/2} \equiv (2/q) \equiv 1 \pmod q$. Since $q \equiv 1 \pmod 3$ we have $3^{(q-1)/2} \equiv (3/q) \equiv -1 \pmod q$. It follows that

$$\tau^q \equiv \bar{\tau} \pmod q \text{ and } \tau^{q+1} \equiv \tau\bar{\tau} \equiv -1 \pmod q.$$

We can prove the theorem. We first prove that $S_{p-1} \equiv 0 \pmod{M_p}$ implies M_p is prime. This part of the proof makes no use of Lemma 2.

From the condition $S_{p-1} \equiv 0 \pmod{M_p}$ we find $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$ so that $\omega^{2^{p-1}} \equiv -1 \pmod{M_p}$ and $\omega^{2^p} \equiv 1 \pmod{M_p}$.

Let l be a prime dividing M_p, and $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$. The coset of ω in $(\mathcal{O}/l\mathcal{O})^*$ has order 2^p by the above congruences.

*This work was partically supported by NSF Grant DMS-8606407.

This content downloaded from 129.82.28.144 on Wed, 02 Dec 2015 13:00:37 UTC
All use subject to JSTOR Terms and Conditions

Suppose l splits in $\mathcal{O}$. Then it follows that

$$(\mathcal{O}/l\mathcal{O})^* \approx (\mathbb{Z}/l\mathbb{Z})^* \times (\mathbb{Z}/l\mathbb{Z})^*,$$

and so 2^p divides $l-1$. Thus, $l = 1 + 2^p k$ for some $k \geqslant 1$. This is impossible because it implies $l \geqslant 1 + 2^p > M_p$.

Suppose l stays prime in $\mathcal{O}$. Then $(\mathcal{O}/l\mathcal{O})^*$ has order $l^2 - 1$ and 2^p divides $l^2 - 1 = (l-1)(l+1)$. If $l \equiv 1 \pmod 4$ we must have 2^{p-1} divides $l-1$, or $l = 1 + 2^{p-1}k$ for some $k \geqslant 1$. This cannot happen since $2l \geqslant 2 + 2^p > M_p$. If $l \equiv 3 \pmod 4$, then 2^{p-1} divides $l+1$ so that $l = -1 + 2^{p-1}k$ for some $k \geqslant 1$. One cannot have $k = 1$ since $2^{p-1} - 1$ does not divide $2^p - 1$. The only possible case is $k = 2$. Then, $l = 2^p - 1 = M_p$, and so M_p is prime.

Finally, suppose M_p is prime. From Lemma 2 we have

$$\tau^{M_p+1} \equiv -1 \pmod{M_p} \quad \text{or} \quad \tau^{2^p} + 1 \equiv 0 \pmod{M_p}.$$

Since $\tau^2 = \omega$, $\omega^{2^{p-1}} + 1 \equiv 0 \pmod{M_p}$. Multiply both sides of this congruence with $\bar{\omega}^{2^{p-2}}$ and recall $\omega\bar{\omega} = 1$. The result is

$$S_{p-1} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}.$$

REFERENCES

1. G. H. Hardy and E. M. Wright, The Theory of Numbers, Oxford at the Clarendon Press, 1965.
2. L. K. Hua, Introduction to the Theory of Numbers, Springer-Verlag, Berlin-Heidelberg-New York, 1982.
3. D. H. Lehmer, On Lucas' test for the primality of Mersenne's numbers, *J. of the London Math. Soc.*, 10 (1935) 162–165.
4. H. Riessel, Prime Numbers and Computer Methods for Factorization, Birkhauser, Boston-Basel-Stuttgart, 1985.
5. W. Sierpinski, Elementary Theory of Numbers, Polski Akademic Nauk., Warsaw, 1964.
6. A. E. Western, On Lucas' and Pepin's tests for the primeness of Mersenne numbers, *J. of the London Math. Soc.*, 7 (1932) 130–137.

The Behaviour of Means Under Equal Increments of Their Variables

J. ACZÉL
Department of Pure Mathematics, University of Waterloo, Waterloo, Ont. Canada N2L 3G1

ZS. PALES
Institute of Mathematics, L. Kossuth University, H-4010 Debrecen, Hungary

In [6], after noting that the arithmetic ($M = A$), geometric ($M = G$), harmonic ($M = H$) means, and the root-mean square (or quadratic mean $M = Q$, denoted in [6] by R) all satisfy

$$M(a_1x, \ldots, a_nx) = M(a_1, \ldots, a_n)x \tag{1}$$

(here and in what follows, except in Proposition 4, $a_1, \ldots, a_n, x$ are supposed to be positive), and

$$A(a_1 + x, \ldots, a_n + x) = A(a_1, \ldots, a_n) + x, \tag{2}$$

This content downloaded from 129.82.28.144 on Wed, 02 Dec 2015 13:00:37 UTC
All use subject to JSTOR Terms and Conditions