A Really Trivial Proof of the Lucas-Lehmer Test

J. W. Bruce

In the paper [1] Rosen gave a beautiful and elementary proof of the Lucas-Lehmer primality test for Mersenne numbers, i.e. those of the form $M_p = 2^p - 1$. This test is very attractive, since it can be easily implemented on a computer, and it gives students the chance of experiencing the thrill of discovering very large (if well-known) primes for themselves. In this article we show that it is possible to simplify Rosen's proof of the sufficiency of the test a little to eliminate any mention of algebraic numbers or questions concerning splittings of primes. In fact we only use a couple of lemmas from group theory, which are hardly worth glorifying with such a description. Of course it is the sufficiency which allows one to produce the large primes, so the half of the result we prove has its attractions. The necessity requires some basic facts concerning quadratic residues. The proof below might make a pleasant application early on in an abstract algebra course. The author was in receipt of a Fulbright award while this note was written.

We start by defining a sequence S_n by setting $S_1 = 4$ and $S_n = S_{n-1}^2 - 2$.

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

We now follow Rosen by setting $\omega = 2 + \sqrt{3}$, $\bar{\omega} = 2 - \sqrt{3}$. One then checks that $\omega\bar{\omega} = 1$ and the next result follows easily by induction:

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

It follows from the lemma that if M_p divides S_{p-1} then $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$. Actually we will want to spell this out explicitly, so we write $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = RM_p$ for some integer R. Multiplying this identity by $\omega^{2^{p-2}}$ we find that

$$\omega^{2^{p-1}} = RM_p\omega^{2^{p-2}} - 1 \qquad (*)$$

and squaring

$$\omega^{2^p} = \left(RM_p\omega^{2^{p-2}} - 1\right)^2 \qquad (**).$$

Now assume that M_p is composite, and choose a prime divisor q with $q^2 \leqslant M_p$. (This is where our proof departs from that of Rosen.) At one stage below we need the fact that q obviously is not 2.

We are going to use some really elementary results and ideas from group theory.

Lemma 2. *Let X be a set with a binary operation which is associative and has an identity. Then the set X^* of invertible elements in X forms a group.*

Proof: Clearly the identity $1 \in X^*$, so we have a non-empty set. We now have only to show that the set X^* is closed under the binary operation. But if x_1 and x_2 are invertible elements with inverses x_1^{-1}, x_2^{-1} then x_1x_2 has inverse $x_2^{-1}x_1^{-1}$.

Lemma 3. *If G is a finite group then the order of an element is at most the order of the group. If $x \in G$ and $x^r = 1$ then the order of x divides r.*

(Results in group theory do not get any easier than this. These results are nowhere near as deep as Lagrange's Theorem for example!)

Proof of Theorem 1: Let Z_q denote the set of integers modulo q, and X denote the set $\{a + b\sqrt{3} : a, b \in Z_q\}$. We can define two binary operations on X, namely addition and multiplication, in the obvious manner. So in the case of multiplication, which is the one of interest, we choose representatives in $Z[\sqrt{3}]$ of our elements of X compute the product in the usual way, $(a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3})$ as $(a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3}$ and then reduce the coefficients modulo q. In the case of addition we obviously get an abelian group, and for multiplication we clearly have an associative (and commutative) binary operation with identity 1. Let X^* denote the group of invertible elements of X with respect to multiplication. Lemma 2 tells us that this is a group, while Lemma 3 tells us that the order of any element of X^* is at most $q^2 - 1$, since X^* contains at least one non-invertible element, namely 0.

Now consider $\omega = 2 + \sqrt{3}$ as an element of X. Since q divides M_p it follows that $RM_p\omega^{2^{p-2}}$, when viewed as an element of X, is 0. So the equalities noted in (*) and (**) above in X reduce to $\omega^{2^{p-1}} = -1$, and $\omega^{2^p} = 1$ respectively. It follows that ω lies in X^*, and has order 2^p. For the order of ω clearly divides 2^p by Lemma 3 and the second equality, but cannot be less than 2^p by the first. So using Lemma 3 again we deduce that $2^p \leq q^2 - 1$. However $q^2 - 1 \leqslant M_p - 1 = 2^p - 2$ and we have a contradiction.

REFERENCE

1. M. I. Rosen, A Proof of the Lucas-Lehmer Test, Amer. Math. Monthly, 95 (1988), 855–856.

Department of Pure Mathematics
The University of Liverpool
L69 3BX, UNITED KINGDOM