THE LUCAS–LEHMER TEST

KEITH CONRAD

1. Introduction

If $2^n - 1$ is prime then n is prime, since

$$n = ab \Longrightarrow 2^n - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

and the factors on the right exceed 1 when $a > 1$ and $b > 1$. When $p \leq 7$ is prime, $2^p - 1$ is prime : $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, and $2^7 - 1 = 127$. But $2^{11} - 1 = 2047 = 23 \cdot 89$, so primality of p is necessary for $2^p - 1$ to be prime but *not* sufficient.

Primes of the form $M_p := 2^p - 1$ are called *Mersenne primes*. It is conjectured that there are infinitely many such primes, but data suggest they are rare: there are over 5.7 million primes $p < 100{,}000{,}000$ and in this range only 51 primes values of M_p have been found. The table below indicates for prime $p \leq 47$ when M_p is prime. A table of all known Mersenne primes is on https://t5k.org/mersenne/.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
M_p prime?	✓	✓	✓	✓		✓	✓	✓			✓				

Using the the equivalences

$$\begin{aligned} 2 \equiv \Box \bmod p &\iff p = 2 \text{ or } p \equiv 1, 7 \bmod 8, \\ 3 \equiv \Box \bmod p &\iff p = 2, 3 \text{ or } p \equiv 1, 11 \bmod 12, \end{aligned}$$

and Euler's criterion $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$, we will derive a primality test for Mersenne primes that is called the Lucas–Lehmer test.

2. Determining primality of Mersenne numbers

The test we give for primality of M_p uses the sequence $\{S_k\}_{k\geq 0}$ where $S_0 = 4$ and $S_k = S_{k-1}^2 - 2$ when $k \geq 1$. It begins 4, 14, 194, and 37634. We will start with a formula for S_k in terms of powers of $2 + \sqrt{3}$ and $2 - \sqrt{3}$.

Lemma 2.1. *Let* $\alpha = 2 + \sqrt{3}$ *and* $\overline{\alpha} = 2 - \sqrt{3}$. *For* $k \geq 0$, $S_k = \alpha^{2^k} + \overline{\alpha}^{2^k}$.

Proof. Let $x_k = \alpha^{2^k} + \overline{\alpha}^{2^k}$. Then $x_0 = \alpha + \overline{\alpha} = 4 = S_0$ and since $\alpha\overline{\alpha} = 1$, for $k \geq 1$ we have

$$x_{k-1}^2 - 2 = (\alpha^{2^{k-1}} + \overline{\alpha}^{2^{k-1}})^2 - 2 = \alpha^{2^k} + 2 + \overline{\alpha}^{2^k} - 2 = \alpha^{2^k} + \overline{\alpha}^{2^k} = x_k,$$

so $x_k = S_k$ for all $k \geq 0$ by induction. □

Theorem 2.2 (Lucas–Lehmer)**.** *For odd primes* p, M_p *is prime* $\iff S_{p-2} \equiv 0 \bmod M_p$.

The proof here, different from the original, is by Rosen [7] for ($\Rightarrow$) and Bruce [1] for ($\Leftarrow$). In both directions we will use modular arithmetic in $\mathbf{Z}[\sqrt{3}]$.

Proof. ($\Longrightarrow$) When M_p is prime, the M_p-th power map in $\mathbf{Z}[\sqrt{3}]/(M_p)$ is additive, so

$$\begin{aligned}(1+\sqrt{3})^{M_p} &\equiv 1+\sqrt{3}^{M_p} \bmod M_p\\ &\equiv 1+\sqrt{3}^{M_p-1}\sqrt{3} \bmod M_p\\ &\equiv 1+(\sqrt{3}^2)^{(M_p-1)/2}\sqrt{3} \bmod M_p\\ &\equiv 1+3^{(M_p-1)/2}\sqrt{3} \bmod M_p.\end{aligned}$$

Since $p \geq 3$, $M_p = 2^p-1 \equiv -1 \equiv 7 \bmod 8$ and $M_p = 2^p-1 = (-1)^p-1 = -2 \equiv 1 \bmod 3$, so $M_p \equiv 7 \bmod 12$. Thus $3 \not\equiv \Box \bmod M_p$ by the rule about when 3 is a square modulo primes, so $3^{(M_p-1)/2} \equiv -1 \bmod M_p$ by Euler's criterion. Thus

$$(1+\sqrt{3})^{M_p} \equiv 1+3^{(M_p-1)/2}\sqrt{3} \equiv 1-\sqrt{3} \bmod M_p. \tag{2.1}$$

We will now calculate $(1+\sqrt{3})^{M_p} \bmod M_p$ in a second way. In $\mathbf{Z}[\sqrt{3}]$,

$$\begin{aligned}(1+\sqrt{3})^{M_p} = (1+\sqrt{3})(1+\sqrt{3})^{M_p-1} &= (1+\sqrt{3})((1+\sqrt{3})^2)^{(M_p-1)/2}\\ &= (1+\sqrt{3})(4+2\sqrt{3})^{(M_p-1)/2}\\ &= (1+\sqrt{3})2^{(M_p-1)/2}(2+\sqrt{3})^{(M_p-1)/2}\\ &= (1+\sqrt{3})2^{(M_p-1)/2}\alpha^{(M_p-1)/2},\end{aligned}$$

where $\alpha = 2+\sqrt{3}$ as in Lemma 2.1. Since $M_p \equiv 7 \bmod 8$, $2 \equiv \Box \bmod M_p$ by the rule about when 2 is a square modulo primes, so $2^{(M_p-1)/2} \equiv 1 \bmod M_p$. Thus

$$(1+\sqrt{3})^{M_p} \equiv (1+\sqrt{3})\alpha^{(M_p-1)/2} \equiv (1+\sqrt{3})\alpha^{2^{p-1}-1} \bmod M_p. \tag{2.2}$$

Combining (2.1) and (2.2),

$$(1+\sqrt{3})\alpha^{2^{p-1}-1} \equiv 1-\sqrt{3} \bmod M_p.$$

Multiply both sides by $1+\sqrt{3}$, with $(1+\sqrt{3})^2 = 4+2\sqrt{3} = 2\alpha$:

$$(2\alpha)\alpha^{2^{p-1}-1} \equiv -2 \bmod M_p.$$

Since M_p is odd, $2 \bmod M_p$ is invertible, so we can cancel the 2 on both sides:

$$\alpha^{2^{p-1}} \equiv -1 \bmod M_p.$$

Write 2^{p-1} in the exponent as $2^{p-2}+2^{p-2}$:

$$\alpha^{2^{p-2}}\alpha^{2^{p-2}} \equiv -1 \bmod M_p.$$

Multiply both sides by $\overline{\alpha}^{2^{p-2}}$. Since $\alpha\overline{\alpha} = 1$,

$$\alpha^{2^{p-2}} \equiv -\overline{\alpha}^{2^{p-2}} \bmod M_p.$$

Thus $\alpha^{2^{p-2}} + \overline{\alpha}^{2^{p-2}} \equiv 0 \bmod M_p$, so $S_{p-2} \equiv 0 \bmod M_p$ by Lemma 2.1. That congruence is in $\mathbf{Z}[\sqrt{3}]$, so $M_p(a+b\sqrt{3}) = S_{p-2}$ for some $a, b \in \mathbf{Z}$. Thus $M_pa = S_{p-2}$ and $M_pb = 0$, so $M_pa = S_{p-2}$, which means $S_{p-2} \equiv 0 \bmod M_p$ in $\mathbf{Z}$.

($\Longleftarrow$) To show M_p is prime, we argue by contradiction. Assume M_p is composite, so it has a prime factor $q \leq \sqrt{M_p}$. Since M_p is odd, q is odd. We will work in $\mathbf{Z}[\sqrt{3}]/(q)$.

Since $S_{p-2} \equiv 0 \bmod M_p$ in $\mathbf{Z}$, $S_{p-2} = M_p N$ for $N \in \mathbf{Z}$, which says $\alpha^{2^{p-2}} + \overline{\alpha}^{2^{p-2}} = M_p N$ by Lemma 2.1. Since $q \mid M_p$, $\alpha^{2^{p-2}} \equiv -\overline{\alpha}^{2^{p-2}} \bmod q$. Multiply both sides by $\alpha^{2^{p-2}}$. Since $\alpha\overline{\alpha} = 1$,

$$\alpha^{2^{p-1}} \equiv -1 \bmod q, \tag{2.3}$$

so $\alpha^{2^p} \equiv 1 \bmod q$. Thus α in $\mathbf{Z}[\sqrt{3}]/(q)$ has order dividing 2^p. The order doesn't divide 2^{p-1} by (2.3)[1], so the order is 2^p. Thus 2^p divides $|(\mathbf{Z}[\sqrt{3}]/(q))^\times| \leq |\mathbf{Z}[\sqrt{3}]/(q)| - 1 = q^2 - 1$, so

$$2^p \leq q^2 - 1 < q^2 \leq M_p = 2^p - 1,$$

which is a contradiction. Thus M_p is not composite, so it is prime. □

Example 2.3. To show $M_{19} = 2^{19} - 1 = 524287$ is prime, the table below lists $S_k \bmod M_{19}$, starting at $k = 2$ so the table fits within the margins, and $S_{17} \equiv 0 \bmod M_{19}$.

k	2	3	4	5	6	7	8	9
$S_k \bmod M_{19}$	194	37634	218767	510066	386344	323156	218526	504140

k	10	11	12	13	14	15	16	17
$S_k \bmod M_{19}$	103469	417706	307417	382989	275842	85226	523263	0

Remark 2.4. The Lucas–Lehmer test is valid with a sequence $\{s_k\}$ where $s_k = s_{k-1}^2 - 2$ and the Jacobi symbols $(\frac{s_0-2}{M_q})$ and $(\frac{-s_0-2}{M_q})$ are 1, such as $s_0 = 4$ and $s_0 = 10$. See Theorem 2.1 in Jansen's PhD thesis https://math.leidenuniv.nl/scripties/PhDJansen.pdf.

Here is some history about the Lucas–Lehmer test. In 1876 Lucas gave (without proof) a sufficient, but not necessary, condition for M_p to be prime if $p \equiv 3 \bmod 4$ [5, Théorème I] and said [4, p. 167] he was able to show M_{127} is prime[2]. In 1878 he gave (again without proof) tests when $p \equiv 1 \bmod 4$ [6, Théorème, p. 316] and $p \equiv 3 \bmod 4$ [6, Théorème II, p. 305]. In 1930, Lehmer [2, Theorem 5.4] showed the primality test given by Lucas for M_p when $p \equiv 1 \bmod 4$ can be sharpened to the necessary and sufficient conditions in Theorem 2.2 and he proved it holds for all primes $p > 2$.

References

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

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

[3] D. H. Lehmer, "On Lucas's test for the primality of Mersenne's numbers," *J. London Math. Soc.*, **10** (1935), 162–165. https://t5k.org/mersenne/LukeMirror/lit/lit_007s.htm.

[4] É. Lucas, "Note sur l'application des séries récurrentes à la recherche de la loi de distribution des nombres premiers," *C. R. Acad. Sci. Paris*, **82** (1876), 165–167. URL https://www.biodiversitylibrary.org/item/24897#page/171/mode/1up.

[5] É. Lucas, "Nouveaux théorèmes d'arithmétique supérieure," *C. R. Acad. Sci. Paris*, **83** (1876), 1286–1288. URL https://www.biodiversitylibrary.org/item/23737#page/1298/mode/1up.

[6] É. Lucas, "Théoriè des fonctions numériques simplement périodiques," *Amer. J. Math.*, **1** (1878), 184–240, 289–321. URL http://edouardlucas.free.fr/oeuvres/Theorie_des_fonctions_simplement_periodiques.pdf

[7] M. I. Rosen, "A proof of the Lucas–Lehmer test," *Amer. Math. Monthly* **64** (1988), 855–856.

[1] Here we are using $q > 2$, since $1 \equiv -1 \bmod 2$.

[2] The number M_{127}, with 39 digits, was the largest known prime until computers were used in the 1950s.