proof of Lucas-Lehmer primality test

The objective of this article is to prove the Lucas-Lehmer primality test:
Let $p>2$ be a prime, and let $M_p=2^p-1$ be the corresponding Mersenne number. Then M_p is prime if and only if M_p divides s_{p-1} (equivalently, if and only if $s_{p-1}\equiv 0\pmod{M_p}$) where the numbers $(s_n)_{n\geq 1}$ are given by the following recurrence relation:

$$\begin{aligned} s_1 &= 4 \\ s_{n+1} &= {s_n}^2-2, \quad n\geq 1 \end{aligned}$$

We show that the validity of the primality test is equivalent to the following theorem, which is then proved directly:

Theorem 1.

(Lucas) M_p is prime if and only if $\alpha^{(M_p+1)/2}\equiv -1\pmod{M_p}$, where $\alpha=2+\sqrt{3}$.

To see that the two are in fact equivalent, let $\beta=2-\sqrt{3}$. Then $\alpha+\beta=4,\quad \alpha\beta=1$. Thus

$$\begin{aligned} s_1 &= \alpha+\beta \\ s_2 &= (\alpha+\beta)^2-2=\alpha^2+\beta^2+2\alpha\beta-2=\alpha^2+\beta^2 \\ s_3 &= \alpha^4+\beta^4 \\ \ldots & \\ s_{p-1} &= \alpha^{2^{p-2}}+\beta^{2^{p-2}} \end{aligned}$$

Note that $2^{p-2}=\frac{M_p+1}{4}$. Then

$$\begin{aligned} s_{p-1}\equiv 0\pmod{M_p} &\Leftrightarrow \alpha^{(M_p+1)/4}+\beta^{(M_p+1)/4}\equiv 0\pmod{M_p} \\ &\Leftrightarrow \alpha^{(M_p+1)/2}+(\alpha\beta)^{(M_p+1)/4}\equiv 0\pmod{M_p} \\ &\Leftrightarrow \alpha^{(M_p+1)/2}\equiv -1\pmod{M_p} \end{aligned}$$

It thus remains to prove Theorem 1. We start with two simple lemmas:

Lemma 2.

If $p>3$ is prime, then $\alpha^{p-1}\equiv 1\pmod{p}$ or $\alpha^{p+1}\equiv 1\pmod{p}$.

Proof.

$$\alpha^p \equiv 2^p + 3^{(p-1)/2}\sqrt{3} \equiv \begin{cases} \alpha \ \ (p) \ \text{ if } \left(\frac{3}{p}\right) = 1 \\ \beta \ \ (p) \ \text{ if } \left(\frac{3}{p}\right) = -1 \end{cases}$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. Thus

$$\left(\frac{3}{p}\right) = 1 \quad \Rightarrow \quad \alpha^{p-1} = \alpha^p\alpha^{-1} = \alpha^p\beta \equiv \alpha\beta = 1 \pmod{p}$$

$$\left(\frac{3}{p}\right) = -1 \quad \Rightarrow \quad \alpha^{p+1} = \alpha^p\alpha \equiv \beta\alpha = 1 \pmod{p}$$

∎

Lemma 3.

Let p be a prime with $p \equiv 7 \pmod{8}$ and $p \equiv 7 \pmod{12}$. Then $\alpha^{(p+1)/2} \equiv -1 \pmod{p}$.

Proof.

$(1+\sqrt{3})^2 = 4 + 2\sqrt{3} = 2\alpha$, so that

$$(1+\sqrt{3})^{p+1} = 2^{(p+1)/2}\alpha^{(p+1)/2}$$

But $p \equiv 7 \pmod{8}$, so that $\left(\frac{2}{p}\right) = 1$. Thus $2^{(p+1)/2} \equiv 2 \cdot 2^{(p-1)/2} \equiv 2 \pmod{p}$ and therefore

$$(1+\sqrt{3})^{p+1} \equiv 2\alpha^{(p+1)/2} \pmod{p}$$

Also,

$$(1+\sqrt{3})^{p+1} = (1+\sqrt{3})(1+\sqrt{3})^p \equiv (1+\sqrt{3})\ (1+3^{(p-1)/2}\sqrt{3}) \pmod{p}$$

But $p \equiv 7 \pmod{12}$, so $3^{(p-1)/2} \equiv -1 \pmod{p}$ and thus

$$(1+\sqrt{3})^{p+1}\equiv(1+\sqrt{3})\ (1-\sqrt{3})=-2\ \ (p)$$

Putting together the two expressions for $(1+\sqrt{3})^{p+1}$, we get $\alpha^{(p+1)/2}\equiv-1\ \ (p)$. ∎

We are now in a position to prove Theorem 1:

Proof.

$(\Rightarrow):$ If M_p is prime where $p>3$ is prime, then note that $M_p\equiv 7\,(8)\,,7\,(1)\,2$ so that M_p satisfies the conditions of Lemma 3. The result follows.

$(\Leftarrow):$ If $\alpha^{(M_p+1)/2}\equiv-1\ \ (M_p)$, choose $q\mid M_p$ for q a prime. Since $M_p\equiv 7\,(1)\,2$, we have $q>3$. Since $\alpha^{(M_p+1)/2}\equiv-1\ \ (M_p)$ also $\alpha^{(M_p+1)/2}\equiv-1\ \ (q)$ and thus $\alpha^{M_p+1}\equiv 1\ \ (q)$. But $M_p+1=2^p$, so

$$\alpha^{2^p}\equiv 1\ \ (q)$$

Thus the order of $\alpha\ \ (q)$ divides 2^n. It can’t divide 2^{n-1} since $\alpha^{(M_p+1)/2}\equiv-1\ \ (q)$, so its order is precisely $2^n=M_p+1$. However, $\alpha^{q+1}\equiv 1\ \ (q)$ or $\alpha^{q-1}\equiv 1\ \ (q)$ by Lemma 2 and thus $q\geq M_p$. But $q\mid M_p$, so $q=M_p$ and M_p is in fact prime. ∎

Title	proof of Lucas-Lehmer primality test
Canonical name	ProofOfLucasLehmerPrimalityTest
Date of creation	2013-03-22 18:42:16
Last modified on	2013-03-22 18:42:16
Owner	rm50 (10146)
Last modified by	rm50 (10146)
Numerical id	5
Author	rm50 (10146)
Entry type	Proof
Classification	msc 11A51