(*February 6, 2010*)

Lucas-Lehmer criterion for primality of Mersenne numbers

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

As of January 2000 or so, the largest prime known was apparently the 38^{th} Mersenne prime, which is the $6,972,593^{th}$ Mersenne number

$$2^{6972593} - 1$$

(Yes, $6,972,593$ is prime.)

[1.1.1] Theorem: *(Lucas-Lehmer)* Define the Lucas-Lehmer sequence L_i by $L_o = 4$ and for $n > 1$ $L_n = L_{n-1}^2 - 2$. Let p be an odd prime p. The Mersenne number $M_p = 2^p - 1$ is prime if and only if

$$L_{p-2} = 0 \bmod M_p$$

A related result much easier to prove is

[1.1.2] Theorem: *(Pepin)* Let n be a positive integer. The Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if

$$3^{\frac{F_n-1}{2}} = -1 \bmod F_n$$

Proof: Suppose that F_n is *not* prime, and let $p < F_n$ be a prime dividing F_n. The assumed congruence modulo F_n implies that also

$$3^{\frac{F_n-1}{2}} = -1 \bmod p$$

from which certainly

$$3^{F_n-1} = +1 \bmod p$$

By Lagrange's theorem, when $g^N = e$ in a group G, the order of g in G is a divisor of N. Here, the group is $(\mathbb{Z}/p)^\times$, g is $3 \bmod p$, and $N = F_n - 1$. Since $N = 2^n$, either the order of 3 in $(\mathbb{Z}/p)^\times$ is $F_n - 1$, or is $(F_n - 1)/2$. But, by the assumed congruence, it is not the latter. Thus, the order of 3 in $(\mathbb{Z}/p)^\times$ is exactly $F^n - 1$. Since the order of the group $(\mathbb{Z}/p)^\times$ is $p - 1$, $F_n - 1$ divides $p - 1$, impossible for $p < F_n$. Thus, the congruence implies the primality of the Fermat number.

For the converse, suppose F_n is prime. Since $(\mathbb{Z}/F_n)^\times$ is cyclic,

$$3^{\frac{F_n-1}{2}} = -1 \bmod F_n$$

if and only if 3 is not a square modulo F_n. (This is *Euler's criterion.*) By quadratic reciprocity, 3 is not a square mod F_n: letting $\left(\frac{a}{p}\right)_2$ be the quadratic symbol, for $n \geq 1$,

$$\left(\frac{3}{F_n}\right)_2 = \left(\frac{F_n}{3}\right)_2 \qquad \text{(since } F_n = 1 \bmod 4 \text{ for } n \geq 1\text{)}$$

$$= \left(\frac{(-1)^{2^n} + 1}{3}\right)_2 = \left(\frac{2}{3}\right)_2 = -1$$

That is, 3 is a non-square mod F_n, so the congruence does hold. ///

[1.1.3] Remark: The groups $(\mathbb{Z}/p)^\times$ and $(\mathbb{Z}/F_n)^\times$ in the proof of Pepin's criterion will be replaced by a somewhat more complicated group in the proof of the Lucas-Lehmer criterion.

Proof: *(of Lucas-Lehmer)* First note that (by induction)

$$\begin{pmatrix} L_n & 0 \\ 0 & L_n \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}^{2^n} + \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}^{-2^n}$$

This observation makes the discussion less surprising.

For a commutative ring R (with 1), let

$$G(R) = \{ \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} : a, b \in R \text{ and } a^2 - 3b^2 = 1 \}$$

Since the determinant is 1, $G(R)$ has inverses:

$$\begin{pmatrix} a & b \\ 3b & a \end{pmatrix}^{-1} = \begin{pmatrix} a & -b \\ -3b & a \end{pmatrix}$$

Thus, $G(R)$ is a group.

Next, we determine the order of the group $G(\mathbb{Z}/q)$ for a prime $q \neq 2, 3$:

$$\text{order}\, G(\mathbb{Z}/q) = q - \left(\frac{3}{p}\right)_2$$

To count the elements of $G(\mathbb{Z}/q)$ is to count the solutions (x, y) in $\mathbb{Z}/q$ to the equation

$$x^2 - 3y^2 = 1$$

since the latter is the condition for

$$\begin{pmatrix} x & y \\ 3y & x \end{pmatrix}$$

to lie in $G(\mathbb{Z}/q)$. For 3 a (non-zero) square mod q, let $\beta^2 = 3 \bmod q$. Then the equation above becomes

$$(x + \beta y)\,(x - \beta y) = 1$$

Since $q \neq 2, 3$, the change of variables

$$u = x + \beta y \quad v = x - \beta y$$

is invertible, converting the equation to

$$u \cdot v = 1$$

Thus, for each non-zero u there is a unique solution v, giving

$$q - 1 = q - \left(\frac{3}{q}\right)_2$$

solutions in that case. On the other hand, for 3 *not* a square modulo q, let β be a square root of 3 in a quadratic field extension K of $\mathbb{Z}/q$. Then

$$x^2 - 3y^2 = N(x + \beta y)$$

where N is the Galois norm from K to $\mathbb{Z}/q$. This norm may be rewritten, using the Frobenius automorphism, as

$$x^2 - 3y^2 = N(x + \beta y) = (x + \beta y)\,(x + \beta y)^q = (x + \beta y)^{q+1}$$

In this case, the elements of $G(\mathbb{Z}/q)$ are exactly the elements $x+\beta y$ of K satisfying

$$(x+\beta y)^{q+1} = 1$$

Since $K^\times$ is cyclic of order q^2-1, there are exactly $q+1$ solutions. Thus, again in this case, we have

$$\mathrm{order}\, G(\mathbb{Z}/q) = q - \left(\frac{3}{p}\right)_2$$

For a *proper* prime divisor q of $M_p = 2^p - 1$, the condition

$$L_{p-2} = 0 \bmod M_p$$

certainly gives

$$L_{p-2} = 0 \bmod q$$

which is equivalent to

$$g^{2^{p-2}} = -g^{-2^{p-2}} \bmod q$$

which gives

$$g^{2^{p-1}} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \bmod q$$

Thus, in the group $G(\mathbb{Z}/q)$,

$$g^{2^p} = 1$$

Then the actual *order* of g, if not 2^p itself, must be a proper divisor of 2^p. We just showed that $g^{2^{p-1}}$ is not the identity. Thus, in the group $G(\mathbb{Z}/q)$,

$$\text{order } g = 2^p \quad (\text{if } q \text{ divides } L_{p-2})$$

On the other hand, by Lagrange's theorem, when q is a proper prime divisor of $M_p = 2^p - 1$, the order of g in $G(\mathbb{Z}/q)$ divides the order of $G(\mathbb{Z}/q)$. That is,

$$2^p \quad \text{divides} \quad q + \left(\frac{3}{q}\right)_2$$

Thus,

$$2^p \le q + \left(\frac{3}{q}\right)_2 \le q+1 < (2^p-1)+1 = 2^p$$

which is impossible. Thus, assuming that $L_{p-2} = 0 \bmod 2^p - 1$, the Mersenne number $M_p = 2^p - 1$ has no proper prime divisor.

Now the converse, that $q = M_p$ prime implies that M_p divides L_{p-2}.

Suppose that $q = M_p = 2^p - 1$ is prime. By quadratic reciprocity, again,

$$\left(\frac{3}{2^p-1}\right)_2 = (-1)^{\frac{(2^p-2)(3-1)}{4}} \left(\frac{2^p-1}{3}\right)_2 = -\left(\frac{(-1)^p-1}{3}\right)_2 = -\left(\frac{-2}{3}\right)_2 = -1$$

so 3 is *not* a square modulo q. Let ρ be a square root of 3 in a quadratic field extension E of $\mathbb{Q}$. Also write ρ for a square root of 3 in an algebraic closure of a finite field $\mathbb{Z}/q$. Identify

$$G(\mathbb{Z}/q) \approx \{x + y\beta : N(x+y\rho) = 1\}$$

and thus view $G(\mathbb{Z}/q)$ as a subgroup of $E^\times$. In either case let σ be the field automorphism which sends ρ to $-\rho$.

Note that q dividing L_{p-2} is equivalent to

$$L_{p-1} = -2 \bmod q$$

since generally $L_n = L_{n-1}^2 - 2$. Also, with $\alpha = 2 + \sqrt{3}$, in the quadratic extension E of $\mathbb{Z}/q$

$$L_n = \alpha^{2^n} + \alpha^{-2^n}$$

so it *suffices* to show that (in E)

$$\alpha^{\frac{q+1}{2}} = -1$$

Since the norm of $\alpha = 2 + \rho$ from E to $\mathbb{Q}$ is 1, by Hilbert's theorem 90 there is $\beta \in E$ such that

$$\alpha = \frac{\beta}{\beta^\sigma}$$

For example, $\beta = 3 + \rho$ will do. Note that the norm $(3 + \rho)(3 - \rho)$ is 6.

We claim that for $a + b\rho$ with $a, b \in \mathbb{Z}$,

$$(a + b\rho)^q = (a + b\rho)^\sigma = a - b\rho \;\; (\text{in } K)$$

To see this, note first that the image ρ^q of ρ under the Frobenius map $\gamma \to \gamma^q$ must be another root of the equation $x^2 - 3 = 0$, and is not equal to ρ (since ρ does not lie in $\mathbb{Z}/q$), so must be $-\rho$. Then compute

$$(a + b\rho)^q = a^q + b^q\rho^q \;\; (\text{in } K)$$

since q divides all the inner binomial coefficients. Then in K

$$(a + b\rho)^q = a^q + b^q\rho^q = a - b\rho = (a + b\rho)^\sigma \;\; (\text{in } K)$$

as claimed. Thus, in particular,

$$(a + b\rho)^{1+q} = (a + b\rho)(a - b\rho) \;\; (\text{in } K)$$

Certainly $3 + \rho \in K$ is not 0, so has a multiplicative inverse in K. In K, compute

$$\alpha = \frac{\beta}{\beta^\sigma} = \frac{\beta}{\beta^q} = \beta^{1-q} = \beta^{-(1+q)} \cdot \beta^2 = (\beta^{1+q})^{-1}\beta^2 = 6^{-1}\beta^2 \qquad (\text{in } K)$$

Taking the $\frac{q+1}{2}^{th}$ power gives

$$\alpha^{\frac{q+1}{2}} = \left(6^{-1}\beta^2\right)^{\frac{q+1}{2}} = \beta^{q+1}\, 6^{\frac{q-1}{2}}\, 6^{-1}$$

since $6^{q-1} = 1 \bmod q$, and this is

$$\alpha^{\frac{q+1}{2}} = 6\left(\frac{6}{q}\right)_2 6^{-1} = \left(\frac{6}{q}\right)_2$$

because the norm of β is 6 and because $6^{(q-1)/2}$ is equal to the quadratic symbol as indicated. Now

$$\left(\frac{6}{q}\right)_2 = \left(\frac{2}{q}\right)_2 \cdot \left(\frac{3}{q}\right)_2 = (+1) \cdot (-1)$$

since $q = 7 \bmod 8$ and by the earlier computation that $(3/q)_2 = -1$.

That is, in K,

$$L_{p-1} = \alpha^{\frac{q+1}{2}} + \alpha^{-\frac{q+1}{2}} = (-1) + (-1) = -2 \bmod q$$

which proves (as noted above) that the primality of $q = 2^p - 1$ implies that q divides L_{p-2}. ///

[1.1.4] Remark: The precise choice of α, apart from the fact that $\alpha\alpha^\sigma = 1$, was irrelevant to the first half of the theorem. Even in the converse, the precise choice of α and β with $\alpha = \beta/\beta^\sigma$ (with *integral* β) played no role until the end, where the fact that the norm of this particular β was 6 implied that $\left(\frac{6}{2^p-1}\right)_2 = -1$ for large odd p. A number-theoretic assessment of possible *other* choices of β with $\alpha = \beta/\beta^\sigma$ shows that a similar conclusion follows in *any* case.

[1.1.5] Remark: Likewise, $\sqrt{3}$ can be replaced by $\sqrt{D}$ with square-free positive D, although this entails complications.

[1.1.6] Remark: A smaller point: from a slightly more sophisticated viewpoint the fact that

$$\beta^\sigma = \beta^q \bmod q$$

follows immediately from the fact that the non-trivial automorphism of $K/\mathbb{Q}$ necessarily reduces modulo q to the Frobenius automorphism of $K/\mathbb{Z}/q$, because in general *decomposition groups* surject to galois groups of residue fields.