

(August 29, 2001)

Lucas-Lehmer criterion for primality of Mersenne numbers

Paul Garrett, garrett@math.umn.edu, ©2001

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

$$2^{6972593} - 1$$

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

Theorem: (*Lucas-Lehmer*) Define the Lucas-Lehmer sequence L_i by $L_0 = 4$ 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

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

A related result which is much easier to prove is

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

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

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

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

from which certainly

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

In general, if $g^N = e$ in a group G , then the order of g in G is either N , or is a proper divisor of N . In the case at hand, the group is $(\mathbf{Z}/p)^\times$, g is $3 \pmod{p}$, and $N = F_n - 1$. Since $N = 2^n$, either the order of 3 in $(\mathbf{Z}/p)^\times$ 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 $(\mathbf{Z}/p)^\times$ is exactly $F_n - 1$. Since the order of the group $(\mathbf{Z}/p)^\times$ is $p - 1$, by Lagrange's theorem $F_n - 1$ divides $p - 1$, which is not possible for $p < F_n$. Thus, we've proven that the congruence implies the primality of the Fermat number.

For the converse, suppose that F_n is prime. Then since $(\mathbf{Z}/F_n)^\times$ is cyclic,

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

if and only if 3 is not a square modulo F_n . (This is sometimes called *Euler's criterion*.) We can verify that indeed 3 is not a square mod F_n by computing via Quadratic Reciprocity, letting $\left(\frac{a}{p}\right)_2$ be the quadratic symbol: for $n \geq 1$,

$$\begin{aligned} \left(\frac{3}{F_n}\right)_2 &= \left(\frac{F_n}{3}\right)_2 \quad (\text{since } F_n = 1 \pmod{4} \text{ for } n \geq 1) \\ &= \left(\frac{(-1)^{2^n} + 1}{3}\right)_2 = \left(\frac{2}{3}\right)_2 = -1 \end{aligned}$$

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

Remark: The groups $(\mathbf{Z}/p)^\times$ and $(\mathbf{Z}/F_n)^\times$ 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 presentation may make the rest of the discussion less surprising.

For a commutative ring R (with 1), let

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

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 $G(\mathbf{Z}/q)$ for a prime $q \neq 2, 3$:

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

To count the elements of $G(\mathbf{Z}/q)$ is nothing other than counting the number of solutions (x, y) in \mathbf{Z}/q to the equation

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

since the latter equation is the condition for

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

to lie in $G(\mathbf{Z}/q)$. If 3 is a (non-zero) square mod q , let $\beta^2 = 3 \pmod{q}$. 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, if 3 is *not* a square modulo q , let β be a square root of 3 in a quadratic field extension K of \mathbf{Z}/q . Then

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

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

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

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

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

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

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

Now, if q is a proper prime divisor of $M_p = 2^p - 1$, the condition

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

certainly gives

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

which is equivalent to

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

which gives

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

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

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

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 $G(\mathbf{Z}/q)$,

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

But, on the other hand, by Lagrange's theorem, continuing to suppose that q is a proper prime divisor of $M_p = 2^p - 1$, the order of g in $G(\mathbf{Z}/q)$ divides the order of $G(\mathbf{Z}/q)$. That is,

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

Thus,

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

which is impossible. Thus, assuming that $L_{p-2} = 0 \pmod{2^p - 1}$, 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 a quadratic reciprocity computation 3 is *not* a square modulo q . Let ρ be a square root of 3 in a quadratic field extension E of \mathbf{Q} . Also write ρ for a square root of 3 in an algebraic closure of a finite field \mathbf{Z}/q . We therefore can identify

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

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

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

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

since generally $L_n = L_{n-1}^2 - 2$. Also, with $\alpha = 2 + \sqrt{3}$, in the quadratic extension E of \mathbf{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 \mathbf{Q} is 1, by Hilbert's theorem 90 there exists $\beta \in E$ such that

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

For example, $\beta = 1 + \rho$ will do. Note that the norm $(1 + \rho)(1 - \rho)$ is -2 .

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

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

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

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

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

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

as claimed. Thus, in particular,

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

Certainly $1 \pm \rho \in K$ is not 0, so has a multiplicative inverse in K . In K , compute

$$\alpha = \frac{\beta}{\beta^\sigma} = \frac{\beta}{\beta^q} = \beta^{1-q} = \beta^{-(1+q)} \cdot \beta^2 = (\beta^{1+q})^{-1} \beta^2 = (-2)^{-1} \beta^2$$

Then taking the $\frac{q+1}{2}$ th power gives

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

since $2^{q-1} = 1 \pmod q$, and this is

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

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

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

since $q = 7 \pmod 8$.

That is, in K ,

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

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

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 $alf = \beta/\beta^\sigma$ (with *integral* β) played no role until there very end, where the fact that the norm of this particular β was -2 implied that $\left(\frac{-2}{2^p-1}\right)_2 = -1$ for all odd p . If some other β were chosen, with norm N , then $q = 2^p - 1$ prime implies (by an identical argument)

$$L_{p-1} = 2 \cdot \left(\frac{N}{q}\right)_2 \pmod{q}$$

Then, in general, we must restrict $q = 2^p - 1$ modulo N or $4N$ (via Quadratic Reciprocity) to assure that $\left(\frac{N}{q}\right)_2 = -1$ and thereby achieve a converse assertion.

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

Remark: It *is* somewhat lucky that $\left(\frac{3}{2^p-1}\right)_2 = -1$ for all odd p , that the unit $\alpha = 2 + \sqrt{3}$ is expressible as β/β^σ with integral β having norm -2 , and $\left(\frac{-2}{2^p-1}\right)_2 = -1$ for all odd prime p . It seems that nearly any other choices, while still yielding a true assertion of the genre of the Lucas-Lehmer criterion, generate many complications.

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

$$\beta^\sigma = \beta^q \pmod{q}$$

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