Lucas-Lehmer primality tests

Let $D \equiv 0$ or $1 \pmod 4$, D not a square, $D \in \mathbb{Z}$.
Let $P \equiv D \pmod 2$ and $Q = \frac{P^2 - D}{4}$, so that $P, Q \in \mathbb{Z}$.

Let $\alpha = \frac{P + \sqrt{D}}{2}$, $\beta = \frac{P - \sqrt{D}}{2}$.

(Then α, β are the roots of the equation
$$x^2 - Px + Q = 0.)$$

The Lucas sequences for P and D are then defined by

$$\frac{V_k + U_k\sqrt{D}}{2} = \alpha^k, \quad k \geq 0.$$

Hence $V_0 = 2$, $V_1 = P$,
$U_0 = 0$, $U_1 = 1$.

Also
$$\frac{V_k - U_k\sqrt{D}}{2} = \beta^k,$$

so
$$V_k = \alpha^k + \beta^k, \quad U_k = \frac{\alpha^k - \beta^k}{\sqrt{D}}.$$

Also we have the recurrence relations

$$\left.\begin{aligned} U_{k+2} &= PU_{k+1} - QU_k \\ V_{k+2} &= PV_{k+1} - QV_k \end{aligned}\right\} \quad k \geq 0.$$

<u>Remark</u> When subsequently applied to Mersenne numbers, we take $D = 12$, $P = 2$, $Q = -2$, $\alpha = 1 + \sqrt{3}$.

Identities

$$V_k^2 - DU_k^2 = 4Q^k$$

$$V_{2k} = V_k^2 - 2Q^k$$

$$V_{2k+1} = V_k V_{k+1} - PQ^k$$

$$U_{2k} = U_k V_k$$

$$V_{k+1} = \frac{1}{2}(PV_k + DU_k)$$

$$U_{k+1} = \frac{1}{2}(V_k + PU_k).$$

$$2U_{k+j} = U_k V_j + U_j V_k$$

$$2V_{k+j} = V_k V_k + DU_k U_j.$$

We work in the ring S_D, consisting of all numbers $\frac{a+b\sqrt{D}}{2}$, where

(i) $a \equiv 0 \pmod 2$ if $D \equiv 0 \pmod 4$,

(ii) $a \equiv b \pmod 2$ if $D \equiv 1 \pmod 4$.

Let N be an odd positive integer. We define congruence in S_D mod N:

$$\gamma_1 \equiv \gamma_2 \pmod N$$

means $\gamma_1 - \gamma_2 = \gamma N$, $\gamma \in S_D$.

Note $\mathbb{Z} \subseteq S_D$ and $\sqrt{D} \in S_D$, as $\sqrt{D} = \frac{0+2\sqrt{D}}{2}$.

Also $\alpha, \beta \in S_D$.

If $\gamma_1 = \frac{a_1 + b_1\sqrt{D}}{2}$ and $\gamma_2 = \frac{a_2 + b_2\sqrt{D}}{2}$, then

$\gamma_1 \equiv \gamma_2 \pmod N \iff a_1 \equiv a_2 \pmod N$ & $b_1 \equiv b_2 \pmod N$.

We say $\gamma \in S_D$ is invertible $(\text{mod } N)$ if $\exists\ \delta$ in S_D such that $\gamma\delta \equiv 1 \pmod N$. We note that if $\gamma\delta' \equiv 1 \pmod N$, then from $(\delta\gamma)\delta' \equiv \delta(\gamma\delta') \pmod N$, we deduce $\delta \equiv \delta' \pmod N$. We write $\delta = \gamma^{-1}$ for any inverse of γ mod N.

THEOREM Suppose $\gcd(N, DQ) = 1$, p an odd prime, p not dividing DQ. Then

(i) $\alpha, \beta, \alpha - \beta$ are invertible mod N;

(ii) $U_k \equiv 0 \pmod N \iff (\alpha\beta^{-1})^k \equiv 1 \pmod N$;

(iii) Let $\gamma \in S_D$. Then

$$\gamma^p \equiv \begin{cases} \gamma \pmod p & \text{if } \left(\frac{D}{p}\right) = 1, \\ \sigma(\gamma) \pmod p & \text{if } \left(\frac{D}{p}\right) = -1. \end{cases}$$

(Here if $\gamma = \frac{a + b\sqrt{D}}{2}$, $\sigma(\gamma) = \frac{a - b\sqrt{D}}{2}$.)

(iv) $U_{p-1} \equiv 0 \pmod p$ if $\left(\frac{D}{p}\right) = 1$,

$U_{p+1} \equiv 0 \pmod p$ if $\left(\frac{D}{p}\right) = -1$.

PROOF Assume $\gcd(N, DQ)=1$.

(i) Let $W \in \mathbb{Z}$, $QW \equiv 1 \pmod{N}$. Then

$$\alpha\beta W = QW \equiv 1 \pmod{N}.$$

Hence α^{-1} and β^{-1} exist $\pmod{N}$.

Also $\alpha-\beta=\sqrt{D}$, $(\alpha-\beta)^{2\phi(N)} = D^{\phi(N)} \equiv 1 \pmod{N}$.

Hence $(\alpha-\beta)^{-1}$ exists mod N.

(ii) $U_k = \dfrac{\alpha^k - \beta^k}{\alpha-\beta}$. Hence as $(\alpha-\beta)^{-1}$ exists mod N, we have

$$U_k \equiv 0 \pmod{N} \Leftrightarrow \alpha^k \equiv \beta^k \pmod{N}$$
$$\Leftrightarrow (\alpha\beta^{-1})^k \equiv 1 \pmod{N}.$$

(iii) Let $\gamma = \dfrac{a+b\sqrt{D}}{2}$ and assume $p \nmid DQ$. Then

$$\begin{aligned}
2\gamma^p \equiv 2^p\gamma^p \equiv (2\gamma)^p &\equiv (a+b\sqrt{D})^p \pmod{p}\\
&\equiv a^p + (b\sqrt{D})^p \pmod{p}\\
&\equiv a^p + b^p\sqrt{D}\,D^{\frac{p-1}{2}} \pmod{p}\\
&\equiv a + b\sqrt{D}\left(\frac{D}{p}\right) \pmod{p}
\end{aligned}$$

Hence

$$\gamma^p \equiv \frac{a+b\left(\frac{D}{p}\right)\sqrt{D}}{2} \pmod{p}.$$

$$= \begin{cases} \gamma & \text{if } \left(\frac{D}{p}\right)=1, \\ \sigma(\gamma) & \text{if } \left(\frac{D}{p}\right)=-1. \end{cases}$$

(iv) (a) Let $\left(\frac{D}{p}\right)=1$. Then $\alpha^p \equiv \alpha \pmod{p}$, so $\alpha^{p-1} \equiv 1 \pmod{p}$. Similarly $\beta^{p-1} \equiv 1 \pmod{p}$. Hence $(\alpha\beta^{-1})^{p-1} \equiv 1 \pmod{p}$ and by part (ii), we have $U_{p-1} \equiv 0 \pmod{p}$.

(b) Let $\left(\frac{D}{p}\right)=-1$. Then

$$\alpha^{p+1} \equiv \alpha^p \alpha \equiv \sigma(\alpha)\alpha \equiv \beta\alpha \pmod{p}$$

Also $\beta^{p+1} \equiv \alpha\beta \pmod{p}$. Hence $(\alpha\beta^{-1})^{p+1} \equiv 1 \pmod{p}$ and by part (ii), we have $U_{p+1} \equiv 0 \pmod{p}$.

<u>COROLLARY</u> (Lucas pseudoprime test)

Let N be an odd integer, $D = P^2 - 4Q$, $\gcd(N, PQ) = 1$, $\left(\frac{D}{N}\right) = -1$, $D \equiv 0$ or $1 \pmod{4}$. Then N is composite if $U_{N+1} \not\equiv 0 \pmod{N}$.

<u>DEFINITION</u> If N is odd and N divides U_{N+1}, but N is composite, N is called a Lucas pseudoprime.

<u>REMARK</u> In practice, one finds the least $|D|$ such that $D \equiv 1 \pmod{4}$ and $\left(\frac{D}{N}\right) = -1$. Then we take $P=1$, $Q = \frac{1-D}{4}$. If $U_{N+1} \equiv 0 \pmod{N}$ and N also passes the base 2 strong pseudoprime test, there is a very good chance that N is prime. This is the test lucas(N) used in CALC.

THEOREM (Lucas-Lehmer primality test)

Let N be odd, $\gcd(N, DQ)=1$ and suppose

(i) $\left(\frac{D}{N}\right)=-1$, (ii) $U_{N+1} \equiv 0 \pmod{N}$,

(iii) $\gcd(U_{\frac{N+1}{q}}, N)=1$ for all primes q dividing $N+1$.

Then N is a prime.

PROOF Suppose N satisfies (i), (ii) and (iii). Let r be a prime factor of N satisfying $\left(\frac{D}{r}\right)=-1$.

Then $U_{N+1} \equiv 0 \pmod{N}$ implies

$$(\alpha\beta^{-1})^{N+1} \equiv 1 \pmod{r}. \qquad (1)$$

Let k be the least positive integer such that $(\alpha\beta^{-1})^k \equiv 1 \pmod{r}$. Then (1) implies $k \mid N+1$.

But $U_{\frac{N+1}{q}} \not\equiv 0 \pmod{r}$ implies $(\alpha\beta^{-1})^{\frac{N+1}{q}} \not\equiv 0 \pmod{r}$ if q is a prime dividing $N+1$. Hence $k=N+1$.

But $U_{r+1} \equiv 0 \pmod{r}$, so $(\alpha\beta^{-1})^{r+1} \equiv 1 \pmod{r}$.

Hence $N+1 \mid r+1$, so $N+1 \leq r+1$. and $N \leq r$.

But $r \mid N$, so $r \leq N$ & hence $r=N$.

To apply this theorem to Mersenne numbers we need the following two lemmas:

LEMMA 1

$$V_{p-\left(\frac{D}{p}\right)} \equiv 2\,Q^{\frac{1-\left(\frac{D}{p}\right)}{2}} \pmod{p},$$

if p is an odd prime not dividing QD.

PROOF

$$2^{p-1}(V_p + U_p\sqrt{D}) = (P+\sqrt{D})^p$$
$$= P^p + \binom{p}{1}P^{p-1}\sqrt{D} + \cdots + \binom{p}{p-1}P(\sqrt{D})^{p-1} + \sqrt{D}^{\,p}$$

Hence
$$2^{p-1}V_p \equiv P^p \pmod{p},$$
$$2^{p-1}U_p \equiv D^{\frac{p-1}{2}} \pmod{p}.$$

Hence
$$V_p \equiv P \pmod{p},$$
$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}.$$

Now
$$2V_{p+1} = V_p P + D U_p \equiv P^2 + D\left(\frac{D}{p}\right) \pmod{p}.$$

Then

(i) $\left(\frac{D}{p}\right) = -1 \Rightarrow 2V_{p+1} \equiv P^2 - D \equiv 4Q \pmod{p},$
$\Rightarrow V_{p+1} \equiv 2Q \pmod{p}$

(ii) $\left(\frac{D}{p}\right) = -1 \Rightarrow 2Q\,V_{p-1} = V_p P - D U_p$
$\equiv P^2 - D \equiv 4Q \pmod{p}$
$\Rightarrow V_{p-1} \equiv 2 \pmod{p}$

LEMMA 2 Let p be an odd prime not dividing DQ. Then

$$V_{\frac{p-\left(\frac{D}{p}\right)}{2}} \equiv 0 \pmod{p} \Leftrightarrow \left(\frac{Q}{p}\right) = -1.$$

PROOF In the identity $V_i^2 = V_{2i} + 2Q^i$, let $i = \frac{p-\left(\frac{D}{p}\right)}{2}$. Then by Lemma 1,

$$V^2_{\frac{p-\left(\frac{D}{p}\right)}{2}} \equiv 2Q^{\frac{1-\left(\frac{D}{p}\right)}{2}} + 2Q^{\frac{p-\left(\frac{D}{p}\right)}{2}} \pmod{p}$$

$$\equiv 2Q^{\frac{1-\left(\frac{D}{p}\right)}{2}}\left(1 + Q^{\frac{p-1}{2}}\right) \pmod{p}$$

$$\equiv 2Q^{\frac{1-\left(\frac{D}{p}\right)}{2}}\left(1 + \left(\frac{Q}{p}\right)\right) \pmod{p}.$$

Hence $p \mid V_{\frac{p-\left(\frac{D}{p}\right)}{2}} \Leftrightarrow \left(\frac{Q}{p}\right) = -1.$

COROLLARY (The Lucas-Lehmer primality test for $M_n = 2^n - 1$, $n \geq 3$.)

Let $S_1 = 4$, $S_t = S_{t-1}^2 - 2$ for $t \geq 2$. Then M_n is prime if and only if $M_n \mid S_{n-1}$.

PROOF Consider the Lucas–Lehmer sequence defined by

$$D = 12,\ P = 2,\ Q = -2,\ \alpha = 1+\sqrt{3},\ \beta = 1-\sqrt{3}.$$

Then

$$V_{i+1} = 2V_i + 2V_{i-1},\quad V_0 = 2 = V_1.$$

$$V_{2i} = V_i^2 - 2(-2)^i = V_i^2 - 2^{i+1} \text{ if } i \text{ even.}$$

Take $i = 2^{t-1}$. Then

$$V_{2^t} = V_{2^{t-1}}^2 - 2\times 2^{2^{t-1}},$$

so if $S_t = V_{2^t}/2^{2^{t-1}}$, we have

$$S_1 = 4 \text{ and } S_t = S_{t-1}^2 - 2.$$

$\Rightarrow$. Let $M_n = p$, a prime. Then

$$\left(\frac{D}{p}\right) = \left(\frac{12}{M_n}\right) = \left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

as $M_n \equiv -1 \pmod 8$ and $M_n \equiv 1 \pmod 3$.

Also $\left(\frac{Q}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)(1) = -1.$

Then by Lemma 2, we have

$$p \mid V_{\frac{p+1}{2}} = V_{2^{n-1}} = 2^{2^{n-2}} S_{n-1}, \text{ so } p \mid S_{n-1}.$$

$\Leftarrow$ Suppose $M_n \mid S_{n-1}$. Then $M_n \mid V_{2^{n-1}}$.

Hence $M_n \mid U_{2^n} = U_{2^{n-1}} V_{2^{n-1}}$.

Also $\gcd(M_n, U_{\frac{M_n+1}{2}}) = 1$. For taking

$i = 2^{n-1}$ in the identity

$$V_i^2 - DU_i^2 = 4Q^i = 4(-2)^i$$

shows $\gcd(M_n, U_{2^{n-1}}) = 1$. Hence M_n is prime by the Lucas–Lehmer test, as $\left(\frac{D}{M_n}\right) = -1$.