Mersenne Primes

Definition. A *Mersenne prime* is a prime of the form $2^n - 1$.

- Equivalently, ... of the form $2^p - 1$ where p is a prime.
- Mersenne primes are related to *perfect numbers*. Euler showed that $\sigma(m) = 2m$, where m is even if and only if $m = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are primes.
- The largest known prime is $2^{77232917} - 1$.

The Lucas Primality Test

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Maple's Version

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\dfrac{P^2 - 4}{n}\right) = -1$.
- Make use of the identities, where $n \geq 1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

The Lucas Primality Test

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Suppose $n \equiv 7 \pmod{12}$ is prime. We can take $P = 4$.

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\frac{P^2 - 4}{n}\right) = -1$.
- Make use of the identities, where $n \geq 1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

The Lucas Primality Test

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Suppose $n \equiv 7 \pmod{12}$ is prime. We can take $P = 4$.

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\frac{P^2 - 4}{n}\right) = -1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

$$v_1 = 4, \; v_2 = 14, \; \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \;\; (n \geq 0)$$

The Lucas Primality Test

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

The Lucas-Lehmer Test. ***Let p be an odd prime, and define recursively***

$$L_0 = 4 \quad \textit{and} \quad L_{n+1} = L_n^2 - 2 \textit{ mod } (2^p - 1) \quad \textit{for} \quad n \geq 0.$$

Then $2^p - 1$ is a prime if and only if $L_{p-2} = 0$.

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

The Lucas-Lehmer Test. ***Let p be an odd prime, and define recursively***

$$L_0 = 4 \quad \textit{and} \quad L_{n+1} = L_n^2 - 2 \ \textit{mod}\ (2^p - 1) \quad \textit{for} \quad n \geq 0.$$

Then $2^p - 1$ is a prime if and only if $L_{p-2} = 0$.

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$L_n = v_{2^n}$$

$$N = 2^p - 1 \text{ is a prime} \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

$$D = P^2 - 4Q$$

The Lucas-Lehmer Test. *Let p be an odd prime, and define recursively*

$$L_0 = 4 \quad \text{and} \quad L_{n+1} = L_n^2 - 2 \ \mathit{mod}\ (2^p - 1) \quad \mathit{for} \quad n \geq 0.$$

Then $2^p - 1$ is a prime if and only if $L_{p-2} = 0$.

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime} \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

$$D = P^2 - 4Q$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \ \ (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

($\Longrightarrow$):

- $3^{(N-1)/2} \equiv -1 \pmod{N}$ and $2^{(N-1)/2} \equiv 1 \pmod{N}$
- It suffices to prove $v_{(N+1)/2} \equiv -2 \pmod{N}$.

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

($\Longrightarrow$):

- $3^{(N-1)/2} \equiv -1 \pmod{N}$ and $2^{(N-1)/2} \equiv 1 \pmod{N}$
- It suffices to prove $v_{(N+1)/2} \equiv -2 \pmod{N}$.
- $2 \pm \sqrt{3} = ((\sqrt{2} \pm \sqrt{6})/2)^2$

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

($\Longrightarrow$):

- $3^{(N-1)/2} \equiv -1 \pmod{N}$ and $2^{(N-1)/2} \equiv 1 \pmod{N}$
- It suffices to prove $v_{(N+1)/2} \equiv -2 \pmod{N}$.
- $2 \pm \sqrt{3} = ((\sqrt{2} \pm \sqrt{6})/2)^2$
- $v_{(N+1)/2} = \left(\dfrac{\sqrt{2}+\sqrt{6}}{2}\right)^{N+1} + \left(\dfrac{\sqrt{2}-\sqrt{6}}{2}\right)^{N+1}$

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \ \ (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$(\implies)$:

- $3^{(N-1)/2} \equiv -1 \pmod N$ and $2^{(N-1)/2} \equiv 1 \pmod N$
- It suffices to prove $v_{(N+1)/2} \equiv -2 \pmod N$.
- $2 \pm \sqrt{3} = ((\sqrt{2} \pm \sqrt{6})/2)^2$
- $v_{(N+1)/2} = \left(\dfrac{\sqrt{2}+\sqrt{6}}{2}\right)^{N+1} + \left(\dfrac{\sqrt{2}-\sqrt{6}}{2}\right)^{N+1}$

$$= 2^{-N} \sum_{j=0}^{(N+1)/2} \binom{N+1}{2j} \sqrt{2}^{N+1-2j} \sqrt{6}^{2j}$$

$$= 2^{(1-N)/2} \sum_{j=0}^{(N+1)/2} \binom{N+1}{2j} 3^j$$

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

($\Longrightarrow$):

- $3^{(N-1)/2} \equiv -1 \pmod N$ and $2^{(N-1)/2} \equiv 1 \pmod N$
- It suffices to prove $v_{(N+1)/2} \equiv -2 \pmod N$.
- $2 \pm \sqrt{3} = ((\sqrt{2} \pm \sqrt{6})/2)^2$
- $v_{(N+1)/2} = 2^{(1-N)/2} \sum_{j=0}^{(N+1)/2} \binom{N+1}{2j} 3^j$
- $2^{(N-1)/2} v_{(N+1)/2} \equiv 1 + 3^{(N+1)/2} \equiv -2 \pmod N$ ■

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

($\Longleftarrow$): Note that this is the important direction!

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

($\Longleftarrow$): Note that this is the important direction!

- $(2 \pm \sqrt{3})^2 - 1 = \pm\sqrt{12}\,(2 \pm \sqrt{3})$ (all signs the same)
- $v_n = u_{n+1} - u_{n-1}$ and $u_{m+n} = u_m u_{n+1} - u_{m-1} u_n$
- If $p^e | u_n$ with $e \geq 1$, then

Future Homework

$$u_{kn} \equiv k u_{n+1}^{k-1} u_n \pmod{p^{e+1}} \quad \text{and} \quad u_{kn+1} \equiv u_{n+1}^k \pmod{p^{e+1}}.$$

BEWARE BAD NOTATION

$$p \neq p$$

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

($\Longleftarrow$): Note that this is the important direction!

- $(2\pm\sqrt{3})^2 - 1 = \pm\sqrt{12}\,(2\pm\sqrt{3})$ (all signs the same)
- $v_n = u_{n+1} - u_{n-1}$ and $u_{m+n} = u_m u_{n+1} - u_{m-1} u_n$
- If $p^e | u_n$ with $e \geq 1$, then

$$u_{kn} \equiv k u_{n+1}^{k-1} u_n \pmod{p^{e+1}} \quad \text{and} \quad u_{kn+1} \equiv u_{n+1}^k \pmod{p^{e+1}}.$$

$$u_{(k+1)n} = u_{kn} u_{n+1} - u_{kn-1} u_n = u_{kn} u_{n+1} + u_n (u_{kn+1} - 4u_{kn})$$

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \ \ (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

($\Longleftarrow$): Note that this is the important direction!

- $(2\pm\sqrt{3})^2 - 1 = \pm\sqrt{12}\,(2\pm\sqrt{3})$ (all signs the same)
- $v_n = u_{n+1} - u_{n-1}$ and $u_{m+n} = u_m u_{n+1} - u_{m-1} u_n$
- If $p^e | u_n$ with $e \geq 1$, then

  $u_{kn} \equiv k u_{n+1}^{k-1} u_n \pmod{p^{e+1}}$ and $u_{kn+1} \equiv u_{n+1}^k \pmod{p^{e+1}}$.
- If $p^e | u_n$ with $e \geq 1$, then $p^{e+1} | u_{pn}$.
- $\forall$ primes p, $\exists\ \varepsilon = \varepsilon_p \in \{-1, 0, 1\}$ such that $p | u_{p+\varepsilon}$.

$$v_1 = 4,\ v_2 = 14,\ \ldots \qquad v_{2^{n+1}} = v_{2^n}^2 - 2 \quad (n \geq 0)$$

$$N = 2^p - 1 \text{ is a prime } \iff v_{(N+1)/4} \text{ is divisible by } N$$

$$u_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{\sqrt{12}} \quad \text{and} \quad v_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$$

- $v_n = u_{n+1} - u_{n-1}$ and $u_{m+n} = u_m u_{n+1} - u_{m-1} u_n$
- If $p^e | u_n$ with $e \geq 1$, then $p^{e+1} | u_{pn}$.
- $\forall$ primes p, $\exists\ \varepsilon = \varepsilon_p \in \{-1, 0, 1\}$ such that $p | u_{p+\varepsilon}$.

$$u_0 = 0, \quad u_1 = 1, \quad u_2 = 4, \quad u_3 = 15, \ldots$$

$$u_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 2^{n-2k-1} 3^k, \quad v_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} 2^{n-2k+1} 3^k$$

$$u_p \equiv 3^{(p-1)/2} \equiv \pm 1 \pmod{p} \quad \text{and} \quad v_p \equiv 4 \pmod{p}$$