# 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-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 $L_{p-2} = 0$.***

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

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

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

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

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

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

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

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

( $\Longrightarrow$ ):

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

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

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

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

( $\Longleftarrow$ ): 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**

$$p \neq p$$

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

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

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

( $\Longleftarrow$ ): 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 $p | u_{p+\varepsilon}$.

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

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

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

- $v_n = u_{n+1} - u_{n-1}$ 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 $p | u_{p+\varepsilon}$.

$$u_0 = 0, \quad u_1 = 1, \quad u_2 = 4, \quad u_3 = 15, \ldots \quad (\varepsilon_2 = \varepsilon_3 = 0)$$

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

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

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

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

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

- $v_n = u_{n+1} - u_{n-1}$ 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 $p | u_{p+\varepsilon}$.

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

$$u_{p-1} \equiv 4u_p - u_{p+1} \equiv 4u_p - v_p - u_{p-1} \equiv -u_{p-1} \pmod{p}$$

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

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

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

- $v_n = u_{n+1} - u_{n-1}$ 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 $p | u_{p+\varepsilon}$.

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

$$u_{p-1} \equiv 4u_p - u_{p+1} \equiv 4u_p - v_p - u_{p-1} \equiv -u_{p-1} \pmod{p}$$

$$u_{p+1} \equiv 4u_p - u_{p-1} \equiv 4u_p + v_p - u_{p+1} \equiv -u_{p+1} \pmod{p}$$

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

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

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

- $v_n = u_{n+1} - u_{n-1}$ 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 $p | u_{p+\varepsilon}$.
- $\gcd(u_n, u_{n+1}) = 1$ and $\gcd(u_n, v_n) \leq 2$

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = P u_n - Q u_{n-1} = 4u_n - u_{n-1}$$

$$v_0 = 2, \quad v_1 = P = 4, \quad v_{n+1} = 4v_n - v_{n-1}$$

$$D u_n = 2v_{n+1} - P v_n \implies 6u_n = v_{n+1} - 2v_n$$

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

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

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

- $v_n = u_{n+1} - u_{n-1}$ and $u_{m+n} = u_m u_{n+1} - u_{m-1} u_n$
- If $p^e | u_n$ with $e \ge 1$, then $p^{e+1} | u_{pn}$.
- $\forall$ primes $p$, $\exists\ \varepsilon = \varepsilon_p \in \{-1, 0, 1\}$ such that $p | u_{p+\varepsilon}$.
- $\gcd(u_n, u_{n+1}) = 1$ and $\gcd(u_n, v_n) \le 2$
- For $m \in \mathbb{Z}^+$, if $\alpha = \alpha(m)$ is minimal such that $u_\alpha \equiv 0 \pmod{m}$, then $u_n \equiv 0 \pmod{m} \iff \alpha | n$.

If $p^e | u_n$ with $e \ge 1$, then

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

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

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

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

- $v_n = u_{n+1} - u_{n-1}$ 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 $p | u_{p+\varepsilon}$.
- $\gcd(u_n, u_{n+1}) = 1$ and $\gcd(u_n, v_n) \leq 2$
- For $m \in \mathbb{Z}^+$, if $\alpha = \alpha(m)$ is minimal such that $u_\alpha \equiv 0 \pmod{m}$, then $u_n \equiv 0 \pmod{m} \iff \alpha | n$.
- $v_{2^{p-2}} \equiv 0 \pmod{N} \implies u_{2^{p-2}} \not\equiv 0 \pmod{N}$

**BEWARE WE'RE BACK TO p BEING p.**

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

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

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

- $v_n = u_{n+1} - u_{n-1}$ 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 $p | u_{p+\varepsilon}$.
- $\gcd(u_n, u_{n+1}) = 1$ and $\gcd(u_n, v_n) \leq 2$
- For $m \in \mathbb{Z}^+$, if $\alpha = \alpha(m)$ is minimal such that $u_\alpha \equiv 0 \pmod{m}$, then $u_n \equiv 0 \pmod{m} \iff \alpha | n$.
- $v_{2^{p-2}} \equiv 0 \pmod{N} \implies u_{2^{p-2}} \not\equiv 0 \pmod{N}$
- $u_{2n} = u_n v_n \implies u_{2^{p-1}} \equiv 0 \pmod{N} \implies \alpha(N) = 2^{p-1}$

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

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

- 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 $p | u_{p+\varepsilon}$.
- For $m \in \mathbb{Z}^+$, if $\alpha = \alpha(m)$ is minimal such that $u_\alpha \equiv 0 \pmod{m}$, then $u_n \equiv 0 \pmod{m} \iff \alpha | n$.
- $u_{2n} = u_n v_n \implies u_{2^{p-1}} \equiv 0 \pmod{N} \implies \alpha(N) = 2^{p-1}$

Write $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ with $p_j$ distinct primes and $e_j \geq 1$. Set $\varepsilon_j = \varepsilon_{p_j}$ and $k = \operatorname{lcm}\{p_j^{e_j - 1}(p_j + \epsilon_j) : j = 1, \ldots, r\}$. Then $u_k \equiv 0 \pmod{N}$. Thus, $\alpha(2^p - 1) = 2^{p-1}$ divides $k$. Hence, $2^{p-1}$ divides $p_j^{e_j - 1}(p_j + \epsilon_j)$ for some $j$. For such $j$, $p_j \geq 2^{p-1} - 1$. Then $3p_j > 2^p - 1$, implying $N$ is prime. $\blacksquare$

# Other Primality Tests

**Theorem (Selfridge-Weinberger).** *Assume that the Extended Riemann Hypothesis holds. Let $n$ be an odd integer $> 1$. A necessary and sufficient condition for $n$ to be prime is that for all positive integers $a < \min\{70(\log n)^2, n\}$, we have $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$ with at least one occurrence of $-1$.*

Note: Primes pass this test but 1729 does not.

**Theorem (Lucas).** *Let $n$ be a positive integer. If there is an integer $a$ such that $a^{n-1} \equiv 1 \pmod{n}$ and for all primes $p$ dividing $n-1$ we have $a^{(n-1)/p} \not\equiv 1 \pmod{n}$, then $n$ is prime.*

**Theorem (Lucas).** ***Let $n$ be a positive integer. If there is an integer $a$ such that $a^{n-1} \equiv 1 \pmod{n}$ and for all primes $p$ dividing $n-1$ we have $a^{(n-1)/p} \not\equiv 1 \pmod{n}$, then $n$ is prime.***

**Revised Theorem.** ***Let $n$ be a positive integer. Suppose that for each prime $p$ dividing $n-1$, there is an $a \in \mathbb{Z}$ such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/p} \not\equiv 1 \pmod{n}$. Then $n$ is prime.***

**Note: Primes pass this test but 1729 does not.**

**This test is good if and only if one can factor $n-1$.**

**Idea: If $p^e \| (n-1)$, then $p^e | \mathrm{ord}_n a \Longrightarrow p^e | \phi(n) \Longrightarrow n$ prime.**