The Lucas-Lehmer Test and Primality Tests of the Form $k2^n \pm 1$

Alaka Ravi

July 12, 2026

Table of Contents

Mersenne Numbers

Definition

Mersenne numbers are numbers of the form

$$2^n - 1,$$

where n is a positive integer.

Mersenne Numbers

Definition

Mersenne numbers are numbers of the form

$$2^n - 1,$$

where n is a positive integer.

Definition

Mersenne primes are Mersenne numbers which are prime.

Example

$2^2 - 1 = 3$, $2^3 - 1 = 7$,$2^5 - 1 = 31$,$2^7 - 1 = 127$

Significance of the Lucas-Lehmer Test

Largest prime known: $2^{136,279,841} - 1$
This number has $41,024,320$ digits

This number was found by the Great Internet Mersenne Prime Search (GIMPS) in October, 2024

- Founded in 1996 by George Woltmann

Properties of Mersenne Numbers

Theorem

If a Mersenne number $M_n = 2^n - 1$ is prime, then n is prime.

Properties of Mersenne Numbers

Theorem

If a Mersenne number $M_n = 2^n - 1$ is prime, then n is prime.

Proof.

We proceed by contradiction. Suppose n is composite. Then, there exists two positive integers greater than 1, a, b such that $ab = n$. We see

$$M_n = 2^{ab} - 1$$
$$= (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + ... + 2^a + 1).$$

Since a and b are both greater than 1, both factors in the final expression for M_n are greater than 1, and thus M_n is composite, a contradiction. ■

Converse is not true! $2^{11} - 1 = 89(23)$

Another Property

Definition

A natural number n is a perfect number if the sum of its divisors excluding n itself equals the n. An example is $6 = 1 + 2 + 3$

Theorem

The natural number n is an even perfect number if and only if n is the form $2^{p-1}M_p$, *where* $M_p = 2^p - 1$ *is a prime.*

Intro to the Lucas-Lehmer test

Lemma

Let the sequence $\{S_i\}$ *be defined as the following:*

$$S_i = \begin{cases} 4 & \text{if } i = 1 \\ S_{i-1}^2 - 2 & \text{if } i > 1 \end{cases}$$

Setting $w = 2 + \sqrt{3}$ *and* $\bar{w} = 2 - \sqrt{3}$,

$$S_i = w^{2^{i-1}} + \bar{w}^{2^{i-1}}.$$

Intro to the Lucas-Lehmer test

Lemma

Let the sequence $\{S_i\}$ be defined as the following:

$$S_i = \begin{cases} 4 & \text{if } i = 1 \\ S_{i-1}^2 - 2 & \text{if } i > 1 \end{cases}$$

Setting $w = 2 + \sqrt{3}$ and $\bar{w} = 2 - \sqrt{3}$,

$$S_i = w^{2^{i-1}} + \bar{w}^{2^{i-1}}.$$

Theorem (Lucas-Lehmer Test)

Let $\{S_i\}$ be the sequence defined as earlier. For an odd prime p, $M_p = 2^p - 1$ is prime if and only if $S_{p-1} \equiv 0 \pmod{M_p}$

Example

Example

Consider the Mersenne prime $2^3 - 1 = 7$.
$S_1 = 4$
$S_2 = S_1^2 - 2 = 14 = 7(2)$.

Sketch of Proof

If $S_{p-1} \equiv 0 \pmod{M_p}$, then M_p is prime.

Proceed using Contradiction. There exists some smallest prime divisor q. Work in $X = \{a + b\sqrt{3} : a, b \in \mathbb{F}_q\}$, with multiplication defined as $(a + b\sqrt{3})(c + d\sqrt{3}) = [(ac + 3bd) \pmod{q}] + \sqrt{3}[(ad + bc) \pmod{q}$. Let X^* be the subset of X in which every element has an inverse.

Recall that setting $w = 2 + \sqrt{3}$ and $\bar{w} = 2 - \sqrt{3}$, $S_i = w^{2^{i-1}} + \bar{w}^{2^{i-1}}$.

We can show that $ord(w) = 2^p$

Noting $|X^*| \leq q^2 - 1$. Since order of an element less than or equal to size of group, and that q is smallest prime factor, we see
$2^p - 1 \leq q^2 - 1 < q^2 \leq M_p = 2^p - 1$

Sketch of Proof

(Converse) If M_p is prime, then $S_{p-1} \equiv 0 \pmod{M_p}$

We can show that $3^{\frac{M_p-1}{2}} \equiv -1 \pmod{M_p}$ and that $24^{\frac{M_p-1}{2}} \equiv -1 \pmod{M_p}$.

Work in $X = \{a + b\sqrt{3} : a, b \in F_{M_p}\}$.

We can than obtain that $w^{\frac{M_p+1}{2}} = -1$
Multiplying by $\bar{w}^{\frac{M_p+1}{4}} \implies w^{\frac{M_p+1}{2}} \bar{w}^{\frac{M_p+1}{4}} = -\bar{w}^{\frac{M_p+1}{4}}$.
$w\bar{w} = 1 \implies w^{\frac{M_p+1}{4}} + \bar{w}^{\frac{M_p+1}{4}} = 0$
$\implies w^{2^{p-2}} + \bar{w}^{2^{p-2}} = S_{p-1} = 0$
$\implies S_{p-1} \equiv 0 \pmod{M_p}$, as desired.

Time Complexity

Definition

Let $f, g : N \to R_{\geq 0}$. If there exists some $n_o \in Z_{>0}$ and positive constant c such that for all $n \geq n_0$, we have $f(n) \leq cg(n)$, then we say that

$$f(n) = O(g(n))$$

Time Complexity

Definition

Let $f, g : N \to R_{\geq 0}$. If there exists some $n_o \in Z_{>0}$ and positive constant c such that for all $n \geq n_0$, we have $f(n) \leq cg(n)$, then we say that

$$f(n) = O(g(n))$$

- Squaring: Say it requires $O(M(p))$.

Time Complexity

Definition

Let $f, g : N \to R_{\geq 0}$. If there exists some $n_o \in Z_{>0}$ and positive constant c such that for all $n \geq n_0$, we have $f(n) \leq cg(n)$, then we say that

$$f(n) = O(g(n))$$

- Squaring: Say it requires $O(M(p))$.
- Subtraction: This requires $O(p)$.

Time Complexity

Definition

Let $f, g : N \to R_{\geq 0}$. If there exists some $n_o \in Z_{>0}$ and positive constant c such that for all $n \geq n_0$, we have $f(n) \leq cg(n)$, then we say that

$$f(n) = O(g(n))$$

- Squaring: Say it requires $O(M(p))$.
- Subtraction: This requires $O(p)$.
- Reduction mod M_p: Reduce n. Letting the last p digits in binary be represented by r, we can write n as $n = k2^p + r$, with $0 \leq r < 2^p$, and integer k.
  $n \equiv k + r \pmod{M_p}$. $\implies$ Modulo reduction requires $O(p)$.

Each iteration requires $O(M(p))$, $p - 2$ iterations $\implies O(pM(p))$ is required.

Fast Fourier Transform Multiplication $\implies O(p^2 logploglogp)$.

"Standard" Multiplication $\implies O(p^3)$

Lucas Sequences

Definition

There are two types of Lucas sequences, depending on fixed integers P and Q: Lucas sequences of the first kind, $U_n(P, Q)$, and Lucas sequences of the second kind, $V_n(P, Q)$, both satisfying the following relation: $x_n = Px_{n-1} - Qx_{n-2}$ but differ on their initial values. $U_0(P, Q) = 0$ and $U_1(P, Q) = 1$, while $V_0(P, Q) = 2$ and $V_1(P, Q) = P$.

Theorem

Let α and β be the roots of

$$x^2 - Px + Q = 0$$

. $V_n = a^n + b^n$ and $U_n = \frac{a^n - b^n}{a - b}$.

Prerequisite Knowledge for Riesel Test

Definition

Let a be an integer, and p be an odd prime. The Legendre symbol, $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if a is a quadratic residue modulo p and } a \not\equiv 0 \pmod{p} \\ -1 \text{ if a is a quadratic non residue modulo p} \\ 0 \text{ if } a \equiv 0 \pmod{p} \end{cases}$$

Definition

Let a be an integer, and n be a positive odd integer, such that for primes $p_1, ...p_m$, and integers $b_1, .., b_m$, where m is a positive integer, $n = p_1^{b_1}...p_m^{b_m}$ The Jacobi symbol $\left(\frac{a}{n}\right)$ is defined as follows:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{b_1} ... \left(\frac{a}{p_b}\right)^{b_m}.$$

Lucas-Lehmer-Riesel Test

Theorem

Let n be an integer greater than 1, and let h be an odd integer such that $0 < h < 2^{n+1} - 1$. Write $N = h2^n - 1$ and let $S1 = V_h(P, 1)$ for some integer P satisfying $\left(\frac{P-2}{N}\right) = 1$ and $\left(\frac{P+2}{N}\right) = -1$. The subsequent terms of the sequence $\{Si\}$ follow $S_{i+1} = Si^2 - 2$. N is prime if and only if $S_{n-1} \equiv 0 \pmod{N}$.

Proth's Test

Definition

A Proth number is a number of the form

$$N = h2^n + 1,$$

for an odd h such that $0 < h < 2^n$.

Proth's Test

Definition

A Proth number is a number of the form

$$N = h2^n + 1,$$

for an odd h such that $0 < h < 2^n$.

Theorem (Proth's Theorem)

Let N be a Proth number. N is prime if and only if there exists a integer a such that $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Fermat Numbers

Definition

Let k be a non-negative integer. A Fermat number is a number of the form $2^{2^k} + 1$.

Fermat Numbers

Definition

Let k be a non-negative integer. A Fermat number is a number of the form $2^{2^k} + 1$.

Definition

A Fermat prime is a prime Fermat number.

Theorem

Let n be a positive integer, and let $N = 2^n + 1$. If N is prime, $n = 2^k$ for some non-negative k

Fermat Numbers

Definition

Let k be a non-negative integer. A Fermat number is a number of the form $2^{2^k} + 1$.

Definition

A Fermat prime is a prime Fermat number.

Theorem

Let n be a positive integer, and let $N = 2^n + 1$. If N is prime, $n = 2^k$ for some non-negative k

Theorem

Let $F_k = 2^{2^k} + 1$, for some positive k. N is prime if and only if

$$3^{\frac{F_k - 1}{2}} \equiv -1 \pmod{F_k}$$

Thank you very much!

I hope you learned something interesting!!