ON THE LUCAS-LEHMER TEST AND PRIMALITY TESTS OF THE FORM $k2^n \pm 1$

ALAKA RAVI

ABSTRACT. This paper presents an overview of the Lucas-Lehmer test, a primality test for Mersenne numbers, alongside primality tests for integers of similar forms. After developing a background in abstract algebra, number theory, and Mersenne numbers, the paper will discuss and present a proof of the Lucas-Lehmer test and analyze its time complexity. This paper will then briefly introduce Lucas sequences before showing a proof of the Lucas-Lehmer Riesel Test. The paper will end with Proth's test and a short exposition on Fermat numbers.

1. INTRODUCTION

In his *Disquistiones Arithmeticae*, Carl Gauss wrote, "The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic... the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated..." [5]

The question of whether any given integer is prime has been studied for thousands of years, and in the process, many primality tests have been developed. These tests can broadly be separated into two types: deterministic and probabilistic.

- Deterministic Primality Tests: These tests provide always determine correctly whether or not an integer is prime. A few examples are the AKS primality test and Eliptic Curve Primality Proving. Both of these are general algorithms, so they don't require numbers of a specific form (unlike the tests presented in this paper). The second of these tests is generally more efficient for large numbers, but the worst case time complexity is unknown, unlike for AKS, which is in polynomial time [1].
- Probabilistic Primality Tests: These tests may have false positives, that is, they might report a composite as prime. Some examples are the Braillie-PSW test and the Miller-Rabin test. The advantage of these tests, despite not being deterministic, is that they are typically faster, making them more useful for practical purposes such as cryptography.

All the primality tests discussed in this paper are of the first kind.

The central focus of this expository paper is the Lucas-Lehmer test, a primality test for Mersenne numbers. These numbers are of the form $2^n - 1$, for a positive integer n. Numbers of this form were studied since antiquity; indeed, Euclid first proved a relationship between Mersenne primes and even perfect numbers [3]. In 1644, Marin Mersenne, the mathematician who these primes are named after, made a list of some Mersenne primes with exponents less than or equal to 257. The exponents for those primes he listed were $2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ [9]. There were errors in the list, however. The Mersenne numbers with exponents of 67 and 257 are in fact composite, while the Mersenne numbers

with exponent 61, 89, and 107 are prime but were not included in the list [6]. In the mid 18th century, Euler proved that the converse of Euclid's theorem was true, around 2000 years later [4].

In the late 19th century, Édouard Lucas proposed sufficient conditions for the primality of Mersenne Numbers, that would lay the early foundation of the Lucas-Lehmer test. He did not prove these tests [8]. In 1930, Derrik Henry Lehmer established, with proof, the modern Lucas-Lehmer test, which gave necessary and sufficient conditions for whether a certain Mersenne number is prime. The statement of this test is mentioned below.

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

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

For an odd prime p, $M_p = 2^p - 1$ is prime if and only if $S_{p-1} \equiv 0 \pmod{M_p}$ [7].

The speed of this primality test plays a major role in its importance, with a time complexity of $O(p^2 log ploglog p)$. This makes the Lucas-Lehmer test enormously useful for finding larger and larger primes.

We also look at the Lucas-Lehmer-Riesel Test in this paper. This was developed by Hans Riesel in the latter half of the 20th century. The test generalizes the Lucas-Lehmer test to numbers of the form $h2^n - 1$. The statement will be ommited here due to the technicalities of the theorem, but will be described later in the paper [13].

We will end by discussing Proth's test and an important special case. The statement of the Proth's test is as follows:

Let N be a number of the form

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

for an odd h such that $0 < h < 2^n$. N is prime if and only if there exists an a such that $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ [10].

2. Great internet Mersenne Prime Search

The Great Internet Mersenne Prime Search is a collaborative volunteer computing project founded in 1996 by George Woltman, with the goal of looking for Mersenne primes. Until 2008, they used primarily the Lucas-Lehmer test. Beginning in 2008, the group started using probabilistic primality tests, and then used the Lucas-Lehmer test confirm if something were a false positive or not.

Due to the speed of the Lucas-Lehmer test, the current largest known prime is a Mersenne prime, found in 2024. The prime is $2^{136279841} - 1$, which is $41,024,320$ digits. Among the 18 Mersenne primes they found by October 2024, 16 of them were world record holders when they were found [6].

3. Background

3.1. **Preliminaries in Algebra.** We begin with a definition of a group.

Definition 3.1. A set G equipped with a binary operation $*$ is a group if

- G is closed under $*$ (for all $a, b \in G$, $a * b \in G$).
- G is associative under $*$ (for all $a, b, c \in G$, $(a * b) * c = a * (b * c)$)
- G contains a unique identity element (There exists an element e such that, for every $a \in G$, $a * e = e * a = a$.

- For every $a \in G$, there exists an inverse a^{-1}, such that $a * a^{-1} = a^{-1} * a = e$.

An example of a group is the integers under addition.

Definition 3.2. Let G be a group, and $a \in G$. The order of a is the smallest positive integer $n \geq 1$ such that $a^n = e$, where e is the identity element. If no such n exists, then a has infinite order. We denote the order of a as $ord(a)$

The order of G is the cardinality of G, or the number of elements in G. Denote the order of G by $|G|$.

Lemma 3.3. *Let G be a finite group and H be a subgroup (a subset that is also a group itself) of G. Let $g \in G$ Denote the left coset $gH = \{gh \mid h \in H\}$. Define the mapping:*

$$\phi : H \to gH,$$

by $\phi(h) = gh$. This mapping is bijective.

Proof. This mapping is surjective by the definition of gH. This mapping is injective, since if $gh = gh'$, multiply on the left by the inverse of g to obtain $h = h'$. ■

Theorem 3.4 (Langrange's Theorem)**.** *Let G be a finite group and H be a subgroup of G. $|H|$ divides $|G|$.*

Proof. By the lemma, there exists a bijective mapping between gH and H, so $|gH| = |H|$. Now we show that any pair of these sets are either disjoint or the same. If $g_1H \cap g_2H \neq \emptyset$, then there exists $h_1, h_2 \in H$ such that $g_1h_1 = g_2h_2$. Multiplying by inverses and noting that H is closed since H is a subgroup we obtain $g_2^{-1}g_1 = h_2h_1^{-1} \in H$. There then exists some $c \in H$ such that $g_1 = g_2c$. We thus obtain

$$g_1H = g_2cH \tag{3.1}$$

We now show that $cH = H$. Since $c \in H$, $cH \subseteq H$. By the lemma, there exists a bijection between cH and H, so $|cH| = |H|$, and since $cH \subseteq H$, we have $cH = H$ Substituting $cH = H$ into 3.1, we obtain $g_1H = g_2H$.

It follows that any two distinct left cosets are disjoint.

The union of these left cosets also forms the entire set. Since H is a subgroup, H contains the identity e. Thus, for any $a \in G$, we have $a \in aH$.

It follows that we can write G as the union of distinct left cosets. By the lemma, there exists a bijection between each coset and H, and so each coset has the same cardinality as H. If m of these cosets form G, we then find $|G| = m|H|$, implying $|H|$ divides $|G|$. ■

Theorem 3.5. *Let G be a finite group, and let $g \in G$, so that g has finite order n in G. Define the cyclic subgroup generated by g as $< g >= \{g^k \mid k \in Z\}$. $| < g > |$ is equal to the order of g.*

Proof. Denote e as the identity. Consider the set $S=\{e, g^1, g^2, ..., g^{n-1}\}$. For any $0 \leq i < j \leq n-1$, we cannot have $g^i = g^j$, for if it did, then multiplying by g^-i yields $g^{j-i} = 1$, which is a contradiction to g having order n. S also consists of all elements in $< g >$. Given an integer k, by the Euclidean algorithm, there exists a integer c and an integer r where $0 \leq r \leq n-1$ such that $k = cn + r$ and thus $g^k = g^{nc}g^r = g^r \in S$. We see thus that $| < g > | = |S| = n$. ■

Theorem 3.6. *Let G be a finite group, and $g \in G$ have finite order. The order of g divides $|G|$.*

Proof. Since $< g >$ is a subgroup, Lagrange's theorem reveals that $| < g > |$ divides $|G|$. Since $| < g > |$ is equal to the order of g, the theorem directly follows. ■

Theorem 3.7. *Let G be a group, e be identity element, and $g \in G$ have finite order n. If k is a positive integer such that $g^k = e$, n divides k.*

Proof. By the Euclidean algorithm, there exist non-negative integers c and integer $0 \leq r \leq n-1$ such that $k = cn + r$. We see thus that $g^k = g^{cn}g^r = g^r = e$. If $r \neq 0$, this contradicts that n is the order of g. Thus r=0, and n divides k. ■

We now discuss fields. Most proofs will be omitted due to length.

Definition 3.8. A field F is a set equipped with two binary operations addition and multiplication such that

- F under addition is a commutative group .
- $F \setminus \{0\}$ under multiplication is a commutative group.
- Multiplication is distributive over addition.

Theorem 3.9. *Fields have no zero divisors. That is, for a field F, for $a, b \in F$,if $ab = 0$, either $a = 0$ or $b = 0$*

Proof. Suppose a is non zero. Then, a has an inverse, so mulitplying by that inverse gives $b = (a^{-1})(0) = 0$. On the other hand, if $a = 0$, then clearly the conditions of the theorem are satisfied. ■

Theorem 3.10. *Let F_p denote the integers modulo a prime p. F_p is a field, called a prime field.*

Definition 3.11. Let F be a field. Denote $F[x]$ to be the set of polynomials with coefficients in F.

Definition 3.12. Let F be a field, and $f(x) \in F[x]$ such that $f(x)$ has degree greater than 0. $f(x)$ is irreducible if it cannot be written as $g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials of degree greater than 0.

Definition 3.13. Let F be a field, and let $f(x), g(x), h(x) \in F[x]$. Define the relation $g(x) \sim h(x)$ if and only if $f(x)$ divides $g(x) - h(x)$. Define the set $\frac{F[x]}{(f(x))}$ as the set of all equivalence classes.

Theorem 3.14. *Let F be a field, and $f(x)$ be a irreducible polynomial. $\frac{F[x]}{(f(x))}$ is a field.*

Definition 3.15. We say a field F has characteristic p if the smallest positive number of copies of the multiplicative identity element that will sum to the additive identity element is p. If no such positive p exists, we say F has characteristic 0.

Theorem 3.16 (Freshman's Dream)**.** *Let p be a prime, and F be a field of characteristic p, For $x, y \in F$, $(x + y)^p = x^p + y^p$*

Theorem 3.17 (Fermat's Little Theorem)**.** *Let F be a field of characteristic p. For $x \in F_p \subseteq F$, we have $x^p = x$.*

3.2. **Number Theory Preliminaries.**

Definition 3.18. An integer n is a quadratic residue modulo m if there exists some integer x such that

$$x^2 \equiv n \pmod{m}$$

Definition 3.19. Let a be an integer, and p be an odd prime. The Legendre symbol, $\left(\frac{a}{p}\right)$ is defined as follows:

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

Lemma 3.20. *Let p be an odd prime, and a be a quadratic residue mod p, and let r satisfy the congruence $x^2 \equiv a \pmod{p}$. The only solutions for x are $x \equiv r \pmod{p}$ and $x \equiv -r \pmod{p}$.*

Proof. Both r and $-r$ clearly satisfy $x^2 \equiv a \pmod{p}$. Conversely, if $x^2 \equiv a \equiv r^2 \pmod{p}$, we have $x^2 - r^2 = (x + r)(x - r) \equiv 0 \pmod{p}$. Since integers modulo p form a field, and fields have no zero divisors, $x \equiv r$ or $x \equiv -r$. ■

Theorem 3.21 (Euler's Criterion)**.** *Let p be an odd prime and a be a integer such that p does not divide a. We have*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}.$$

Proof. Let k and l be integers. If p does not divide k. Then, $kx \equiv l \pmod{p}$ has a unique solution modulo p. A solution exists, since k has an inverse because $gcd(p, k) = 1$. This solution is unique, for if there was some x' satisfying the condition, we see

$$k(x - x') \equiv 0 \pmod{p}.$$

Since p does not divide k, by Euclid's lemma, it follows that $p \mid x - x'$, and that $x \equiv x' \pmod{p}$.

We then do the following. For each residue non zero residue y whose square is not a, we define x such that $x \equiv y^{-1} \pmod{p}$ so that $xy \equiv a \pmod{p}$, and we can group these residues into pairs (x, y). If a is a quadratic non-residue, then these pairs partition the $p-1$ non zero residues. This is because no $y \equiv x \pmod{p}$, for if so then $y^2 \equiv a \pmod{p}$, contradicting that a is a quadratic residue. Multiplying each pair, we obtain a. Thus, multiplying all the non zero residues gives

$$(p - 1)! \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

By Wilson's theorem, $(p - 1)! \equiv -1 \pmod{p}$, which gives the desired result for quadratic non-residues. On the other hand, if a is a quadratic residue, we pair the residues similarly, ignoring those residues whose square is a. By the lemma, those residues are some integers r and $-r$ whose product forms $-a$ instead of a. We thus obtain $-1 \equiv (p - 1)! \equiv -a^{\frac{p-1}{2}} \pmod{p}$, implying the desired results for quadratic residues,

$$1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

■

Theorem 3.22. *The Legendre symbol is completely multiplicative. That is, for integers a and b, and odd prime p,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. This follows directly from Euler's criterion. If $p \nmid a$ and $p \nmid b$, we have

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} \pmod{p} \\ &\equiv (a)^{\frac{p-1}{2}}(b)^{\frac{p-1}{2}} \pmod{p} \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.\end{aligned}$$

Since the Legendre symbol only outputs -1 or 1, and $-1 \not\equiv 1 \pmod{p}$ since p is an odd prime, we obtain

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)..$$

On other hand, if p divides either a or b, both sides of the equality in the desired theorem become 0, so the theorem remains true. ■

Theorem 3.23 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.$$

Proof. Due to length, we will neglect the proof here. ■

Theorem 3.24. *Let p be an odd prime. Exactly half of non-zero residues of p are quadratic residues.*

Proof. Consider $x, y \in \{1, ..., (\frac{p-1}{2})\}$, where $x \not\equiv y$. We show that $x^2 \equiv y^2 \mod p$, by contradiction. Suppose $x^2 \equiv y^2 \pmod{p}$. We then see $(x+y)(x-y) \equiv 0 \pmod{p}$. Since integers modulo a prime are a field, and fields have no 0 divisors, $p \mid x+y$ or $p \mid x-y$. Since $x \not\equiv y$, $p \mid x+y$. However, $1 \leq x+y \leq p-1$, so $p \nmid x+y$, a contradiction.

Now we show that $\{1^2, ..., (\frac{p-1}{2})^2\}$ consists of all non zero quadratic residues. For any residue a, $(-a)^2 \equiv a^2 \pmod{p}$. We note $a \not\equiv -a \pmod{p}$, since if $2a \equiv 0 \pmod{p}$, due to p being odd, $p \mid a$, contradicting that a is non zero. It follows that for every non zero quadratic residue mod p, there exists two elements in $F_p \setminus 0$ whose square gives that quadratic residue. If there were more than $\frac{p-1}{2}$ non zero quadratic residues, it follows then there would be more $p-1$ elements in $F_p \setminus 0$, but that is clearly not the case. ■

Now we will discuss the Jacobi symbol, a generalization of the Legendre symbol that can have a non prime bottom argument. When the bottom argument is an odd prime, the symbol is equivalent to the Legendre symbol.

Definition 3.25. 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:

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

Theorem 3.26. *Letting $\left(\right)$ denote the Jacobi symbol, for an integer a and positive odd integer n, if $\left(\frac{a}{n}\right) = -1$, a is a quadratic non residue modulo n.*

Proof. Suppose a is a quadratic residue modulo n. Then, there exists some integer x such that $x^2 \equiv a \pmod{n}$. Write n such that for primes $p_1, ...p_m$, and integers $b_1, .., b_m$, where m is a positive integer, $n = p_1^{b_1}...p_m^{b_m}$. It follows that, for each prime p_i, $1 \leq i \leq m$, $x^2 \equiv a \pmod{p_i}$, and thus that $\left(\frac{a}{p_i}\right) = 1$. Expanding out the Jacobi symbol in terms of prime divisors of n, we obtain $\left(\frac{a}{n}\right) = 1$, a contradiction. ■

We mention that if n is composite, unlike for prime n, if $\left(\frac{a}{n}\right) = 1$, it is not necessarily true that a is a quadratic residue modulo n;

Theorem 3.27. *Holding either the bottom or top argument fixed, the Jacobi symbol is completely multiplicative in the other argument.*

Proof. Multiplicity in the top argument follows directly from using the definition of the Jacobi symbol, then the fact that Legendre's symbol is completely multiplicative.

Multiplicity in the bottom argument follows directly from the definition of the Jacobi symbol. ■

3.3. **Mersenne numbers and Basic Properties.**

Definition 3.28. Mersenne numbers are numbers of the form

$$2^n - 1,$$

where n is a positive integer.

Definition 3.29. Mersenne primes are Mersenne numbers which are prime.

We will begin by discussing some basic yet interesting properties of Mersenne primes relating to divisibility.

Theorem 3.30. *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 a, b such that $ab = n$. We see

$$\begin{aligned} M_p &= 2^{ab} - 1 \\ &= (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + ... + 2^a + 1). \end{aligned}$$

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. ■

It's important to iterate that the converse of this theorem is not true. That is, if n is prime, it is not true that $2^n - 1$ is prime. A clear counterexample of this is $2^{11} - 1 = 2047 = 89(23)$ Another interesting property of Mersenne numbers arises when considering the prime factors of a Mersenne number with a prime exponent.

Theorem 3.31. *Let p be an odd prime and suppose $M_p = 2^p - 1$. Any prime factor of M_p is of the form $2kp + 1$, where k is a positive integer.*

Proof. Let q be a prime factor of M_p, so that

$$2^p \equiv 1 \pmod{q}.$$

Denote m as the multiplicative order of 2 modulo q, and we see that m divides p, but since p is prime, $m = p$. Moreover, since the order of an element divides the order of the group, we obtain that $p = m$ divides $q - 1$, so there exists some positive integer c such that $cp = q - 1$. Since M_p is odd, q is odd and thus $q - 1$ is even. Combining that with the hypothesis that p is odd, we see c is even, so there exists some positive integer k such that $c = 2k$. We thus obtain $2kp = q - 1$,from which the theorem directly follows. ■

Theorem 3.32. *Let p be an odd prime. For any prime factor q of $2^p - 1$,*

$$q \equiv \pm 1 \pmod{8}.$$

Proof. This proof will use the second supplementary law of quadratic reciprocity, which states that for any odd prime p, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } -1 \pmod{8} \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8} \end{cases}$$

By the previous theorem, there exists some positive integer k such that $q = 2pk + 1$. We see, with the second equality using that $2^p \equiv 1 \pmod{q}$, that

$$\begin{aligned} 2^{\frac{q-1}{2}} &\equiv 2^{pk} \pmod{q} \\ &\equiv 1 \pmod{q}. \end{aligned}$$

It follows by Euler's criterion that

$$\left(\frac{2}{q}\right) = 1,$$

and by the law stated in the beginning of this proof, that $q \equiv \pm 1 \pmod{8}$ ■

The next theorem deals with when Mersenne numbers divide each other.

Theorem 3.33. *Let a and b be positive integers such that $a < b$. Let $M_a = 2^a - 1$, and $M_b = 2^b - 1$. M_a divides M_b if and only if a divides b.*

Proof. Suppose M_a divides M_b. We see

$$2^b \equiv 1 \pmod{2^a - 1}.$$

By the Euclidean algorithm, there exists a positive integer k and integer r so that $0 \leq r < a$, where

$$b = ak + r.$$

Substituting, we obtain

$$2^{ak}2^r \equiv 1 \pmod{2^a - 1}.$$

Since $2^a \equiv 1 \pmod{2^a - 1}$, we see

$$2^r \equiv 1 \pmod{2^a - 1}.$$

We see thus that $2^a - 1 \mid 2^r - 1$, but since $0 \leq r < a$, the divisibility is only possible when $r = 0$, from which we obtain $b = ak$.

Conversely, if a divides b, there exists a positive integer k so that b=ak. We see, by using the fact that $2^a \equiv 1 \pmod{2^a - 1}$ for the second equality, that

$$\begin{aligned} 2^b - 1 &\equiv 2^{ak} - 1 \pmod{2^a - 1} \\ &\equiv (1)^k - 1 \pmod{2^a - 1} \\ &\equiv 0 \pmod{2^a - 1}, \end{aligned}$$

implying $M_a \mid M_b$, as desired. ■

Theorem 3.34. *Let, for any positive integer k, $M_k = 2^k - 1$. For any positive integers a and b,*

$$gcd(M_a, M_b) = M_{gcd(a,b)}.$$

Proof. Let $d = gcd(a, b)$. By 3.33, since $d \mid a$ and $d \mid b$, we see $M_d \mid M_a$ and $M_d \mid M_b$, from which it follows $M_d \mid gcd(M_a, M_b)$.

Now, let c be an arbitrary common factor of M_a and M_b. Since $2^a \equiv 1 \pmod{c}$ and $2^b \equiv 1 \pmod{c}$, we note

$$ord_c(2) \mid d.$$

It follows that $2^d \equiv 1 \pmod{c}$, which shows $c \mid 2^d - 1$. Since c was an arbitrary common factor of M_a and M_b, $gcd(M_a, M_b) \mid M_d$. Combining this with $M_d \mid gcd(M_a, M_b)$, we obtain $gcd(M_a, M_b) = M_d = M_{gcd(a,b)}$, as desired. ■

The final property we will cover deals with the relationship between Mersenne numbers and even perfect numbers. A natural number n is a perfect number if the sum of its divisors excluding n itself equals n. An example is $6 = 1 + 2 + 3$.

Theorem 3.35. *The natural number n is an even perfect number if and only if n is of the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is a prime.*

Proof. This proof will use the fact that, denoting $\sigma(n)$ to be the sum of divisors of n, including n itself, for relatively prime integers a, b, $\sigma(ab) = \sigma(a)\sigma(b)$.

Suppose $n = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is prime. We note $gcd(2^{p-1}, 2^p - 1) = 1$ by Bezout's identity, since $2(2^{p-1}) - 1(2^p - 1) = 1$ We thus see

$$\sigma(n) = \sigma(2^{p-1}(2^p - 1) = \sigma(2^{p-1})\sigma(2^p - 1).$$

$\sigma(2^{p-1}) = 1 + 2 + ... + 2^{p-1} = 2^p - 1$, Moreover, by the hypothesis, $2^p - 1$ is prime, so $\sigma(2^p - 1) = 1 + 2^p - 1 = 2^p$.

Substituting into the expression for $\sigma(n)$, we obtain

$$\sigma(n) = 2^p(2^p - 1).$$

Since σ includes n as a divisor, we subtract n, obtaining that the sum of the divisors of n excluding n is $2^{p-1}(2^p - 1)$, which equals n itself, as desired.

Conversely, suppose n is an even perfect number. We write n in the form $2^k m$, where k is a positive integer, and m is an odd positive integer. Since $\sigma(n)$ includes n itself, and since n is perfect,

$$2^{k+1}m = \sigma(2^k m) \tag{3.2}$$

$$= (2^{k+1} - 1)\sigma(m). \tag{3.3}$$

Since $2^{k+1}-1$ is odd, $gcd(2^{k+1}-1, 2^{k+1}) = 1$, so by Euclid's lemma, $2^{k+1}-1$ divides m. Furthermore. since $2^{k+1}-1 > 1$, we have that $\frac{m}{2^{k+1}-1}$ is a divisor of n that is not equal to n. Dividing both sides of 3.3 by $2^{k+1}-1$, we obtain, using σ' to denote any other divisors of m,

$$\begin{aligned}\frac{2^{k+1}m}{2^{k+1}-1} &= \sigma(m) \\ &= m + \frac{m}{2^{k+1}-1} + \sigma' \\ &= \frac{2^{k+1}m}{2^{k+1}-1} + \sigma'.\end{aligned}$$

It follows that $\sigma' = 0$, and since this means there are no other divisors of m, yet 1 must be a divisor, we obtain that m is a prime, and that $\frac{2^{k+1}m}{2^{k+1}-1} = 1$, so that $m = 2^{k+1}-1$, and $n = 2^k(2^{k+1}-1)$, as desired. ■

The forward direction was proven by Euclid, but the converse was proven by Euler over 2000 years later.

The next section will focus on the most efficient test for primality of Mersenne numbers, the Lucas-Lehmer Test. As we remarked earlier, as a result of this test, many of the largest primes we know are Mersenne numbers, but that begs the question: are there an infinite number of Mersenne primes? This question remains unproven.

4. The Lucas-Lehmer Test

We now look at the Lucas-Lehmer Test.

Lemma 4.1. *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 $\bar{w} = 2-\sqrt{3}$,

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

Proof. We proceed by induction. We establish the base case by seeing $S_1 = w^1 + \bar{w}^1 = 4$. Now, suppose $S_{i-1} = w^{2^{i-2}} + \bar{w}^{2^{i-2}}$. Noting $w\bar{w} = (2+\sqrt{3})(2-\sqrt{3}) = 1$, we find that $S_i = S_{i-1}^2 - 2 = w^{2^{i-1}} + 2(w\bar{w})^{2^{i-2}} + \bar{w}^{2^{i-1}} - 2 = w^{2^{i-1}} + \bar{w}^{2^{i-1}}$ ■

Theorem 4.2. *Let $\{S_i\}$ be the sequence defined in 4.1. For a odd prime p, $M_p = 2^p - 1$ is prime if and only if $S_{p-1} \equiv 0 \pmod{M_p}$*

Proof. First we show that if $S_{p-1} \equiv 0 \pmod{M_p}$, M_p is prime. If $S_{p-1} \equiv 0 \pmod{M_p}$, there exists some integer k such that $S_{p-1} = w^{2^{p-2}} + \bar{w}^{2^{p-2}} = kM_p$. Multiplying by $w^{2^{p-2}}$, rearranging, and using the fact that $w\bar{w} = 1$, we obtain

$$w^{2^{p-1}} = kM_p w^{2^{p-2}} - 1 \tag{4.1}$$

Now, we proceed by contradiction. Suppose M_p is not prime. There then exists a smallest prime factor of M_p q, which is greater than 2 since Mersenne numbers are odd. Let

$$X = \{a + b\sqrt{3} : a, b \in \mathbb{F}_q\} = \frac{\mathbb{F}_{\text{ll}}[x]}{x^2 - 3},$$

We define multiplication, for $a, b, c, d \in \mathbb{Z}_{\text{ll}}$, as

$$(a + b\sqrt{3})(c + d\sqrt{3}) = [(ac + 3bd) \pmod q] + \sqrt{3}[(ad + bc) \pmod q.$$

Multiplication in X is closed, associative, and has the identity element 1. Thus, taking the set X^* to be the subset of all elements of X that have an inverse, it follows that X^* is a group under multiplication. Note $|X^*| \leq q^2 - 1$ since $X^* \subseteq X/\{0\}$, and $|X| = q^2$. Since $M_p \equiv 0 \pmod q$, and since $w \in X$ we have, $kM_p w^{2^{p-2}} = 0$ in X. Substituting into 4.1, we obtain

$$w^{2^{p-1}} = -1.$$

Since q is odd, $-1 \neq 1$. Squaring gives

$$w^{2^p} = 1.$$

This shows that w is in X^* since w has an inverse. Since $w^{2^{p-1}} \neq 1$, the order of w divides 2^p but not 2^{p-1}, from which it follows that the order of w is 2^p. Using the fact that the order of any element is less than or equal to the size of the group, $2^p \leq q^2 - 1 < q^2$. Since we defined q as the smallest prime factor of M_p, we see $q^2 \leq 2^p - 1$. We thus obtain

$$2^p < 2^p - 1,$$

a contradiction. This direction of the proof was adapted from J.W. Bruce [2]

Now, we show the converse. Suppose M_p is prime. Note that $2^3 \equiv 8 \pmod{12}$, and if $2^n \equiv 8 \pmod{12}$, $2^{n+2} \equiv 32 \equiv 8 \pmod{12}$, so by induction, for odd $n \geq 3$, $2^n - 1 \equiv 7 \pmod{12}$. By quadratic reciprocity, $\left(\frac{M_p}{3}\right)\left(\frac{3}{M_p}\right) = (-1)^{\frac{3-1}{2}\frac{M_p-1}{2}} = (-1)^{\frac{M_p-1}{2}}$. Since $M_p \equiv 7 \pmod{12}$, $M_p \equiv 3 \pmod 4$ and $M_p \equiv 1 \pmod 3$, we see that $(-1)^{\frac{M_p-1}{2}} = -1$ and $\left(\frac{M_p}{3}\right) = 1$ respectively. It follows that

$$\left(\frac{3}{M_p}\right) = -1$$

By Euler's criterion, we see

$$3^{\frac{M_p-1}{2}} = -1.$$

Since $2^p \equiv 1 \pmod{M_p}$, we see $2 \equiv (2^{\frac{p+1}{2}})^2 \pmod{M_p}$. It follows that 2 is a quadratic residue, so Euler's criterion reveals

$$2^{\frac{M_p-1}{2}} \equiv 1 \pmod{M_p}.$$

We see thus that $24^{\frac{M_p-1}{2}} = 3^{\frac{M_p-1}{2}}(2^{\frac{M_p-1}{2}})^3 \equiv -1 \pmod{M_p}$. Let

$$X = \{a + b\sqrt{3} : a, b \in Z_{M_p}\},$$

and let $\sigma = 2\sqrt{3}$, so that $w = \frac{(6+\sigma)^2}{24}$. Using Freshman's Dream and Fermat's Little theorem, we see that

$$\begin{aligned}(6 + \sigma)^{M_p} &= 6^{M_p} + \sigma^{M_p} \\ &= 6 + 2(3^{\frac{M_p-1}{2}})(\sqrt{3}) \\ &= 6 - \sigma\end{aligned}$$

Using $w = \frac{(6+\sigma)^2}{24}$,we obtain

$$\begin{aligned} w^{\frac{M_p+1}{2}} &= \frac{(6+\sigma)(6+\sigma)^{M_p}}{24 * 24^{\frac{M_p-1}{2}}} \\ &= \frac{-(6+\sigma)(6-\sigma)}{24} \\ &= -1 \end{aligned}$$

Multiplying by $\bar{w}^{\frac{M_p+1}{4}}$, we obtain

$$w^{\frac{M_p+1}{2}} \bar{w}^{\frac{M_p+1}{4}} = -\bar{w}^{\frac{M_p+1}{4}}$$

. Recalling that $w\bar{w} = 1$, we get $w^{\frac{M_p+1}{4}} + \bar{w}^{\frac{M_p+1}{4}} = 0$ Substituting in for $M_p = 2^p - 1$, we obtain

$$w^{2^{p-2}} + \bar{w}^{2^{p-2}} = S_{p-1} = 0,$$

implying that $S_{p-1} \equiv 0 \pmod{M_p}$, as desired. This direction of the proof is a specical case adapted from Öystein Rodseth's more general proof of the Lucas-Lehmer-Riesel test. We also reference Rodseth later in this paper for the proof of the Lucas-Lehmer-Riesel test itself [14] ■

5. Time Complexity

A core reason behind the significance of the Lucas-Lehmer test is the efficiency of the test. We will use big-O notation.

Definition 5.1. 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

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

It's important to be careful with the use of the equal sign, for there can be distinct functions f_1 and f_2 that $f_1(n) = O(g(n))$ and $f_2(n) = O(g(n))$. This is also why we usually keep the function on the left side of the equals sign. Perhaps it is more clear to use set notation, where we can write $f(n) \in O(g(n))$, but using the equals sign is generally more common. There are certain conveniences to using the equal sign, namely with algebraic manipulation. We now look at the time complexity of the Lucas-Lehmer test. We first examine each iteration of the sequence, which involves squaring, subtraction, and reduction mod M_p.

- Squaring: For squaring, we denote complexity of multiplying two p bit integers by $M(p)$. Thus, squaring requires $O(M(p))$, the specifics of which will be examined later.
- Subtraction: This requires $O(p)$.
- Reduction mod M_p: Here, the form of the Mersenne numbers become deeply important. At each iteration, we consider the expansion of the n, the number we want to reduce, in binary. Letting r be the integer represented by the lowest p bits, we can write n as $n = k2^p + r$, for some integer k, where k represents the remaining bits. $2^p \equiv 1 \pmod{M_p}$ so we obtain that $n \equiv k + r$. We note that $0 \leq r < 2^p$. This means that all one must do for the modulo reduction is separating the lowest p bits and addition, both of which require $O(p)$, and so the total modulo reduction also requires $O(p)$.

Since the subtraction and modulo reduction are $O(p)$, multiplication holds the most significance, so each iteration requires $O(M(p))$. Since there are $p-2$ iterations, $O(pM(p))$ is required. Using the standard multiplication algorithm we obtain a total time complexity of $O(p^3)$. Using Fast Fourier Transform based multiplication, we obtain $O(p^2 logploglogp)$ [15].

6. Lucas Sequences

We will use Lucas sequences, in particular Lucas sequences of the second kind, to find the starting value of the generalized Lucas-Lehmer-Riesel test.

Definition 6.1. 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 for $n \geq 2$: $x_n = Px_{n-1} - Qx_{n-2}$ 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 6.2. *Let α and β be the roots of*

$$x^2 - Px + Q.$$

$V_n = \alpha^n + \beta^n$ and $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$.

Proof. For V_n, we confirm the starting value and that the sequence satisfies the recursion. The base cases, $n = 0$ and $n = 1$, yield $V_0 = 2$, and $V_1 = P$a s desired. For the recursion. we see

$$\begin{aligned} V_{n+1} &= \alpha^{n-1}\alpha^2 + \beta^{n-1}\beta^2 \\ &= \alpha^{n-1}(Pa - Q) + \beta^{n-1}(P\beta - Q) \\ &= PV_n - QV_{n-1}. \end{aligned}$$

The second equality follows from substituting α and β into the quadratic.
Now we similarly show this for U_n. $U_0 = 0$ and $U_1 = 1$.

$$\begin{aligned} U_{n+1} &= \frac{\alpha^{n+1} - \beta^{n+1}}{a - b} \\ &= \frac{\alpha^{n-1}\alpha^2 - \beta^{n-1}\beta^2}{\alpha - \beta} \\ &= \frac{\alpha^{n-1}(P\alpha - Q) - \beta^{n-1}(P\beta - Q)}{\alpha - \beta} \\ &= PU_n - QU_{n-1}, \end{aligned}$$

as desired. ∎

6.1. Properties.

We will now discuss a few properties of Lucas sequences.

Theorem 6.3. $V_{2n} = V_n^2 - 2Q^n$

Proof. Recall that $V_n = a^n + b^n$, where a and b are the roots of the characteristic polynomial. We see

$$\begin{aligned} V_n^2 - 2Q^n &= a^{2n} + b^{2n} + 2(ab)^n - 2Q^n \\ &= a^{2n} + b^{2n} \\ &= V_{2n}. \end{aligned}$$

The second equality follows from Vieta's formulas, which imply that $ab = Q$. ∎

The results from this section were taken from Riesel [13].

7. Lucas-Lehmer-Riesel Test

This test is a generalization of the Lucas-Lehmer test.

Theorem 7.1. *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 $S_1 = V_h(P, 1)$ 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 $S_{n-1} \equiv 0 \pmod{N}$ [13].*

Proof. This proof is adapted from Rodseth [14]. Let $D = (P-2)(P+2)$. By multiplicativity of the Jacobi symbol, $\left(\frac{D}{N}\right) = \left(\frac{P-2}{N}\right)\left(\frac{P+2}{N}\right) = -1$, and there is thus some prime p that divides N such that $\left(\frac{D}{p}\right) = -1$. Viewing F_{p^2} as $\frac{F_p[x]}{(x^2-D)}$, which is a field since D is a quadratic non-residue, there exists some σ such that $\sigma^2 = D$. Also let

$$\alpha = \frac{(P + 2 + \sigma)^2}{4(P + 2)}.$$

Since α and α^{-1} are the roots of the characteristic polynomial of this Lucas sequence,

$$V_i = \alpha^i + \alpha^{-i}.$$

Now, by induction, we will show that

$$S_i = \alpha^{h2^{i-1}} + \alpha^{-h2^{i-1}}.$$

The base case, $S_1 = V_h(P, 1)$. Supposing $S_n = \alpha^{h2^{n-1}} + \alpha^{-h2^{n-1}}$, we find $S_{n+1} = \alpha^{h2^n} + \alpha^{-h2^n} + 2(\alpha\alpha^{-1})^{h2^{n-1}} - 2 = a^{h2^n} + a^{-h2^n}$, as desired. By the binomial theorem and Fermat's Little theorem, we see, $(P+2+\sigma)^p = P+2+\sigma^p$. Note that $\sigma^p = \sigma(\sigma^{2(\frac{p-1}{2})}) = \sigma D^{\frac{p-1}{2}} = \sigma\left(\frac{D}{p}\right) = -\sigma$. Substituting, we obtain that

$$(P + 2 + \sigma)^P = P + 2 - \sigma.$$

Furthermore, we see

$$\begin{aligned}
\alpha^{\frac{p+1}{2}} &= \frac{(P + 2 + \sigma)^{p+1}}{(4(P + 2))^{\frac{p+1}{2}}} \\
&= \frac{(P + 2 + \sigma)(P + 2 - \sigma)}{(4(P + 2))^{\frac{p+1}{2}}} \\
&= \frac{(P + 2)^2 - \sigma^2}{(4(P + 2))^{\frac{p+1}{2}}}
\end{aligned}$$

Substituting $\sigma^2 = D = (P - 2)(P + 2)$, we obtain

$$\begin{aligned}
a^{\frac{p+1}{2}} &= \frac{4(P + 2)}{(4(P + 2))^{\frac{p+1}{2}}} \\
&= (4(P + 2))^{-\frac{p-1}{2}}.
\end{aligned}$$

By Euler's Criterion and multiplicative property, we obtain

$$a^{\frac{p+1}{2}} = \left(\frac{P + 2}{p}\right). \tag{7.1}$$

If $S_{n-1} \equiv 0 \pmod{N}$., $S_{n-1} = 0$ in F_{p^2}. Substituting gives $\alpha^{h2^{n-2}} + \alpha^{-h2^{n-2}} = 0$. Multiplying by $\alpha^{h2^{n-2}}$ yields $\alpha^{h2^{n-2}} S_{n-1} = \alpha^{h2^{n-1}} + 1 = 0$. Squaring both sides of $\alpha^{h2^{n-1}} = -1$ reveals that 2^n divides the multiplicative order, in $F^*_{p^2}$, of α. Squaring both sides of 7.1 yields that there exists some $k \geq 1$ such that $p + 1 = k2^n$. Let $N/p = q$ We find then that $h2^n - 1 = N = (2^n k - 1)q$. where q is of the form $2^n m + 1$ for integer m. If N doesn't equal P, $m \geq 1$. If $m = k = 1$, wee see that $h = 2^n$ is even, contradicting that h is odd. It follows that either k or m are greater than or equal to 2. If $m \geq 2$,$h2^n - 1 \geq (2^n - 1)(2^{n+1} + 1) = 2^{2n+1} - 2^n - 1$, from which it follows that $h \geq 2^{n+1} - 1$, contradicting the hypothesis of this theorem. If $k \geq 2$ we see that $h2^n - 1 \geq (2^{n+1} - 1)(2^n + 1) = 2^{2n+1} + 2^n - 1$, from which it too follows that $h \geq 2^{n+1} - 1$.

Conversely, suppose N is prime. Then, $N = p$. We obtain from 7.1 and the hypothesis that $a^{\frac{p+1}{2}} = -1$. Multiplying by $a^{-\frac{p+1}{4}}$ yields $S_{n-1} = 0$, implying $S_{n-1} \equiv 0 \pmod{N}$, as desired. ■

The original Lucas-Lehmer follows as an immediate consequence, putting $h = 1$ and $P = 4$.

8. Proth's Test

We lightly discuss Proth's test and Proth's numbers, due to sharing a similar form to the numbers treated in the Lucas-Lehmer-Riesel test.

Definition 8.1. A Proth number is a number of the form

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

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

Theorem 8.2. *Let N be a Proth number. N is prime if and only if there exists an a such that $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ [10].*

The following proof is adapted from Ribenboim [12].

Proof. Suppose $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$. Let $N = h2^n + 1$, for integers n and h such that $0 < h < 2^n$. Note $N - 1 = h2^n$. Since h is odd, $gcd(h, 2^n) = 1$. In addition, $gcd(a^{\frac{N-1}{2}} - 1, N) = 1$, for if there existed some positive integer d such that $d \mid a^{\frac{N-1}{2}} - 1$ and $d \mid N$, we obtain $d \mid a^{\frac{N-1}{2}} - 1$ and, from the hypothesis, $d \mid a^{\frac{N-1}{2}} + 1$, implying $d \mid 2$. Since N is odd, it follows that $d = 1$. Now, we proceed by contradiction. Suppose N is composite. let p be a prime factor of N, and call o the multiplicative order of a modulo p. Since $-1 \equiv a^{\frac{N-1}{2}} = a^{h2^{n-1}} \pmod{N}$, it follows that $a^{h2^{n-1}} \equiv -1 \pmod{p}$. Squaring both sides yields $a^{h2^n} \equiv 1 \pmod{p}$. Since the integers modulo a prime excluding the 0 element form a group, by 3.7, we have $o \mid h2^n$, but not $o \mid h2^{n-1}$. Thus, since h is odd, $2^n \mid o$. Furthermore, by Fermat's little theorem and again using 3.7, we obtain $o \mid p - 1$., from which we see $2^n \mid p - 1$. There then exists some positive integer m such that $2^n < m2^n + 1 = p$. However, since $0 < h < 2^n$, $N < 2^{2n}$, so $\sqrt{N} < 2^n < p$. Since p was an arbitrary prime divisor, this reveals all prime divisors of N are greater than $\sqrt{N}$, which is only possible if N is prime.

Conversely, suppose N is prime. Since half of non zero residues of N are quadratic non residues, let a be some quadratic non residue modulo N. By Euler's criterion,

$$\begin{aligned} a^{\frac{N-1}{2}} &\equiv \left(\frac{a}{N}\right) \pmod{N} \\ &\equiv -1 \pmod{N}. \end{aligned}$$

■

8.1. **Fermat Numbers.** An interesting special case arises when $h = 1$.

Theorem 8.3 (Pépin's Test)**.** *Let $F_k = 2^{2^k} + 1$, for some positive k. F_k is prime if and only if*

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

[11].

Proof. By Euler's criterion, necessity follows for any a value that is a quadratic non residue, so it is sufficient to show that 3 is a quadratic non-residue.

Since $2^2 \equiv 1 \pmod 3$, and with positive integer n if $2^{2^n} \equiv 1 \pmod 3$, we see $2^{2^{n+1}} = (2^{2^n})^2 \equiv 1 \pmod 3$. It follows by induction that for positive integers n, $2^{2^n} \equiv 1 \pmod 3$. We then obtain that $F_k \equiv 2 \pmod 3$. Since 2 is a quadratic non-residue modulo 3, we obtain $\left(\frac{F_k}{3}\right) = -1$. Also, note that $F_k = 2^{2^k} + 1 \equiv 1 \pmod 4$. By quadratic reciprocity,

$$[\left(\frac{F_k}{3}\right)\left(\frac{3}{F_k}\right) = (-1)^{\frac{3-1}{2}\frac{F_k-1}{2}}$$

Substituting for $\left(\frac{F_k}{3}\right)$ and noting that $F_k = 2^{2^k} + 1 \equiv 1 \pmod 4$, we obtain that $\left(\frac{3}{F_k}\right) = -1$, so 3 is a quadratic non residue modulo F_k, as desired.

■

Theorem 8.4. *Let n be a positive integer, and let $N = 2^n + 1$. If N is prime, $n = 2^k$ for some non-negative k*

Proof. Suppose n has an odd factor not equal to 1. There then exists an odd integer $a > 1$ and integer $k \geq 0$ such that $n = a2^k$. We then reduce modulo $2^{2^k} + 1$, using $2^{2^k} \equiv -1 \pmod{2^{2^k} + 1}$, to obtain $2^{a2^k} + 1 \equiv (-1)^a + 1 \equiv 0 \pmod{2^{2^k} + 1}$. It follows that $2^{2^k} + 1$ divides N, but is neither N or 1, contradicting that N is prime. ■

Definition 8.5. Let k be a non-negative integer. A Fermat number is a number of the form $2^{2^k} + 1$.

Definition 8.6. A Fermat prime is a prime Fermat number.

Fermat conjectured that all Fermat numbers were prime. This is not the case, however. The first 5 (starting from $k = 0$) Fermat numbers are all prime, but when $k = 5$, the number is not prime. The first 5 Fermat numbers are the only ones confirmed prime. The $6th$ to $33rd$ have been confirmed to be composite. It is unknown whether these first 5 Fermat numbers are the only Fermat primes [12].

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

[2] J. W. Bruce. A really trivial proof of the lucas-lehmer test. *The American Mathematical Monthly*, 100(4):370–371, 1993.

[3] Euclid. *The Thirteen Books of Euclid's Elements*. Dover Publications, New York, 2nd edition, 1956. Unabridged republication of the 1925 second edition.

[4] Leonhard Euler. De numeris amicabilibus. *Opuscula varii argumenti*, 2:23–107, 1750.

[5] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Yale University Press, New Haven, CT, 1966.

[6] GIMPS Project. Great internet mersenne prime search. `http://www.mersenne.org/`, 2026.

[7] Derrick H. Lehmer. An extended theory of lucas' functions. *Annals of Mathematics*, 31(3):419–448, 1930.

[8] Édouard Lucas. *Théorie des nombres*, volume 1. Gauthier-Villars, Paris, 1891.

[9] Mersenne, Marin. *Cogitata Physico-Mathematica*. Antoine Bertier, 1644.

[10] François Proth. Théorèmes sur les nombres premiers. *Comptes Rendus de l'Académie des Sciences de Paris*, 85:329–331, 1878.

[11] Théophile Pépin. Sur le nombre et la nature des diviseurs analytiques des nombres de fermat. *Comptes Rendus de l'Académie des Sciences*, 85:356–358, 1877.

[12] Paulo Ribenboim. *The New Book of Prime Number Records*. Springer-Verlag, New York, NY, 3rd edition, 1995.

[13] Hans Riesel. Lucasian criteria for the primality of $n = h2^n - 1$. *Mathematics of Computation*, 23(108):869–875, 1969.

[14] Öystein J. Rodseth. A note on primality tests for $n = h \cdot 2^n - 1$. *BIT Numerical Mathematics*, 34(3):451–454, 1994.

[15] Arnold Schönhage and Volker Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3):281–292, 1971.