DOI: https://dx.doi.org/10.21123/bsj.2023.7791

A Comparative Study between a Novel Deterministic Test for Mersenne Primes and the Well-Known Primality Tests

Yahia Awad [1*] *Ramiz Hindi* [1] *Haissam Chehade* [2,3]

[1] Department of Mathematics and Physics, School of Arts and Sciences, Lebanese International University, Bekaa, Lebanon.
[2] Department of Mathematics and Physics, School of Arts and Sciences, Lebanese International University, Saida, Lebanon.
[3] Department of Mathematics and Physics, School of Arts and Sciences, The International University of Beirut, Beirut, Lebanon.
[*]Corresponding author: yehia.awad@liu.edu.lb
E-mails addresses: r.math090@gmail.com, haissam.chehade@b-iu.edu.lb

Received 18/9/2022, Revised 22/11/2022, Accepted 23/11/2022, Published Online First 20/3/2023, Published 28/10/2023

Abstract:

In this article, we propose a new deterministic primality test for the Mersenne numbers $2^n - 1$ which is introduced by the Hindi Awad test (HAT). The idea of this test is related to that of Pepin's primality test for Fermat numbers $2^{2^n} + 1$. In addition, a modification to solve the weaknesses in the Selfridge-Lucas Test (SLT) is presented and used to suggest a new modified test called Hindi Selfridge-Lucas test (HLT) with the help of base 3. Finally, a comparative study between some well-known primality tests and the new test is done in order to identify and classify them from the least to the most powerful and reliable tests according to their level of strength, speed, and effectiveness based on the results obtained through programs prepared and operated by *Mathematica* where the results are presented through tables and graphs.

Keywords: Deterministic test, Mersenne numbers, Primality test, Probabilistic test, Proth numbers.

Introduction:

Prime numbers have occupied their significance since the beginning of civilization because they form the building blocks of whole numbers. Even today, many researchers try to understand their analogs since there is no valid formula to generate them, and their distribution is still considered mysterious which forms a big puzzle for all researchers and scientists. A primality test is a method used to determine whether an input natural number is prime or composite using some number theoretic rules and theorems. Primality testing is mostly used in the fields of cryptography and cybersecurity [1, 2]. In general, primality tests are different integer factorization because they only state whether a number is prime or not without giving its prime factors of it. In addition, primality testing is considered one of the oldest fundamental problems in mathematics, and it becomes more and more important due to its applications in cryptography such as network cyber security [3, 4].

There are two types of primality tests, deterministic and probabilistic tests. On one hand, a primality test is deterministic if its output is "True" when the number is a prime, yet it is "False" when the input is composite with a hundred percent probability [5]. On the other hand, the primality test is probabilistic which is often called a pseudoprimality test. Furthermore, each primality test has its properties, and it can be applied only to special types of numbers and special algebraic structures. There are many primality tests that can be found in the literature; they are classified according to their algebraic structure and accuracy [3, 6, 7].

In this paper, a comparative study is presented in order to point out the most important and efficient well-known primality tests. In addition, two new approaches for primality tests are introduced: The first approach is the Hindi Awad test (HAT) which is used to test the primality of Mersenne numbers. Its idea is related to that of Pepin's primality test for Fermat numbers. The second approach is the Hindi-Selfridge Lucas test (HLT) which hunts the Lucas pseudoprimes by Lucas sequences with special parameters.

Well-Known Primality Tests:

There is a huge set of strategies and methods which are valid to check and verify the primality of a given positive number based on given algebraic structures. They are classified as either probabilistic or deterministic tests. In the following, the most important and widely used primality tests are presented. For more details, one can see [8] and the references therein.

The Probabilistic Tests

Probabilistic primality tests are algorithms used to output whether an input number is prime or not within a certain probability of error. In this type of primality testing, the algorithm typically picks a random number called (witness) and verifies some criteria involving the tested number. Most probabilistic primality tests declare a witness to be either a definitely composite or a probable prime. A composite number that erroneously passes such a test is called a pseudoprime. There are many well-known probabilistic primality tests for any odd positive integer n that are widely used. The following theorems can be found in [9, 10].

Theorem 1: (**Fermat's Test - FT**) If there exist $a \in Z_n^*$ such that $a^n \not\equiv a(mod\ n)$, then n is composite.

The weakness of **FT** is due to the presence of the pseudoprimes (Carmichael numbers), and its probability error is less than 50% with a running time of $\tilde{O}(k\ log^2 n)$. For more information, one can see [10,] and the references therein.

Theorem 2: (**Solovay-Strassen Test - SST**) If there exists $a \in Z_n^*$ such that $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right)(mod\ n)$, then n is composite where $\left(\frac{a}{n}\right)$ is the Legendre symbol.

The idea of the **SST** test is based on both Fermat's Little Theorem and Euler's Criterion. The weakness of this method is that some of Euler's pseudoprimes may be reported, and its probability error is less than 50%. However, the running time of this method is of order $O(k \log^3 n)$.

Theorem 3: (**Miller-Rabin Test - MRT**) If $n - 1 = 2^j d$ with $j > 1$, d is an odd number, and if there exists
$a \in Z_n^*$ such that $a^d \not\equiv 1\ (mod\ n)$ and $a^{2^r d} \not\equiv -1\ (mod\ n)$ for all $r \in Z_j$, then n is composite.

MRT is also a probabilistic test based on Fermat's Little Theorem with the help of the existence of non-trivial square roots in Z_n. Its weakness is due to some strong pseudoprimes that may be reported, and its running time is of order $O(k \log^3 n)$ with a probability error of less than 25%.

Theorem 4: (**Proth's Test - PT**) If $n - 1 = 2^j d$ with d is odd such that $d < 2^j$, and if there exists a positive integer $a \in Z_n^*$ such that $a^{\frac{n-1}{2}} \not\equiv -1\ (mod\ n)$, then n is prime.

Theorem 5: (**Proth's General Test - PGT**) Let $n = kp^m + 1$ where p is prime and $gcd(k, p) = 1$. If there exists $1 \le j \le m$ such that $\Phi_p\left(a^{kp^{j-1}}\right) \equiv 0\ (mod\ n)$ and $2j > log_p k\ + m$, then n is prime.

It is noted that **PT** and **PGT** are probabilistic primality tests where the first is based on the Pocklington criterion and the second is based on the computation of the cyclotomic polynomials.

The Deterministic Tests

A primality test is deterministic if its output is "True" when the number is prime and "False" when the input is composite with absolute certainty.

Lucas Sequence Primality Testing

This test is considered a generalization for the SST and it is based on a special recursive sequence called Luca's sequence [3, 11]. If P and Q are any integers and if $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$ are the roots of the quadratic equation $x^2 - Px + Q = 0$ whose discriminant $D = P^2 - 4Q$ is positive, then the following relations are obtained:

$$P = \alpha + \beta,\ Q = \alpha\beta, \text{ and } D = (\alpha - \beta)^2.$$

Assume that $D \equiv 0\ (mod 4)$, or $D \equiv 1\ (mod 4)$. Then, the Lucas sequence is defined by the following two recursive sequences: $\{U_n(P, Q)\}$ and $\{V_n(P, Q)\}$ with $n \ge 0$ such that

$$U_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ and } V_n(P, Q) = \alpha^n + \beta^n. \qquad 1$$

For simplicity and without losing generality, the use of $U_n = U_n(P, Q)$ and $V_n = V_n(P, Q)$ is significant. It can be noted that for $n \ge 2$, $U_n = PU_{n-1} - QU_{n-2}$ and $V_n = PV_{n-1} - QU_{n-2}$ with $U_0 = 0$, $U_1 = 1$ and $V_0 = 2$, $V_1 = P$. Special numbers may be obtained from Lucas's sequence (1) such as Fibonacci numbers for $P = 1$ and $Q = -1$, and Mersenne numbers for $P = 3$ and $Q = 2$.

The proofs of the following theorem and corollary can be found in [11].

Theorem 6: (**Lucas Theorem**) Consider the integers P and Q and the Lucas sequence $\{U_n\}_{n \ge 0}$ defined in Eq.1. If p is an odd prime with $p \nmid Q$ and $\left(\frac{D}{p}\right) = -1$, then $U_{p+1} \equiv 0\ (modp)$.

Corollary 1: (**Lucas Test**) Let n be an odd positive integer such that $\delta(n) = n - \varepsilon(n)$ where $\varepsilon(n) = \left(\frac{D}{n}\right)$. If $n \nmid U_{\delta(n)}$ and $\varepsilon(n) = -1$ with $gcd(n, Q) = 1$, then n is composite.

Definition 1: (**Lucas Pseudoprimes**) Any composite number n with $n \nmid Q$ satisfying $U_{\delta(n)} \equiv 0 \ (mod \ n)$ is called a Lucas pseudoprime.

For example, if $n = 5559$ with $P = 3$ and $Q = -1$, then $D = 13$ and the sequence generated by $\{U_{5559}\}$ has the form $\{0, 1, 3, 10, 33, 109, 360, 1189, \ldots., 2617\}$. The Jacobi symbol $\left(\frac{5559}{13}\right) = -1$ and $U_{5559} \equiv 0 \ (mod \ n)$. Nonetheless, this number can be written in this form $5559 = 3 \times 17 \times 109$, and hence 5559 is a Lucas pseudoprime. However, if $n = 19$ with $P = 3$ and $Q = -1$, then $\left(\frac{19}{13}\right) = -1$ and $U_{20} \equiv 0 \ (mod \ n)$. Thus, 19 is Lucas probable prime.

Now, in order to modify the above method, P and Q should be chosen more effectually and rapidly such that $\left(\frac{D}{n}\right) = -1$. The first method is proposed by Selfridge when $P = Q = 1$ [11]. It is based on skipping -3 from the odd numbers as a consequence of the appearing periodic results first, then selecting D to be the first element in $\{5, -7, 9, -11, \ldots\}$ such that $gcd(D, n) = 1$ and $\left(\frac{D}{n}\right) = -1$. In this case, $P = 1$ and $Q = (1 - D)/4$. For example, if $n = 5559$, which is Carmichael number, then Selfridge's method selects $D = 13$ and $\{P, Q\} = \{1, -3\}$. This modifies that $U_{5560} \not\equiv 0 \ (mod \ n)$ and hence n is composite. However, for $n = 2017$, which is prime, the method selects $D = 5$ and $\{P, Q\} = \{1, -1\}$ which gives that $U_{2018} \equiv 0 (modn)$ and implies that 2017 is prime. The second method is suggested by Baillie [12]. It is based on selecting the discriminant D as the first element in the sequence of the odd positive numbers with common difference 4 and $\left(\frac{D}{n}\right) = -1$. Then, P is selected to be the least odd number greater than $D^{\frac{1}{2}}$ and $Q = (P^2 - D)/4$. For example, if $n = 5559$, it selects $D = 13$ and $\{P, Q\} = \{3, -1\}$ where the Lucas test fails.

It is well known that the results obtained by the Selfridge-Lucas test (**SLT**) are weak. The SLT cannot be considered a good deterministic method for hunting primes because some composite numbers (Lucas pseudoprimes) satisfy Corollary 1. This study suggests a new approach that can be used to solve this problem by doing some modifications on **SLT** to present a new modified test called **Hindi Selfridge Lucas test** (**HLT**) with the help of **FLT using** base 3. Also, the selection of the Lucas sequence criteria and D are based on Selfridge's method [11, 12].

The following lemma can be found in [11].

Lemma 1: If n is odd and $\{U_n\}_{n\geq 0}$ is a Lucas sequence so that $\left(\frac{D}{n}\right) = -1$ and $n | U_{n+1}$, then $gcd(n, QD) = 1$.

Proof: Assume that $p | gcd(n, QD)$. Then, $D = P^2 - 4Q = P^2 - 4(kp) \equiv P^2 \not\equiv 0 \ (mod \ p)$ which implies that $p \nmid D$ and $\nmid P$. Consider the sequence $U_n = PU_{n-1} - QU_{n-2}$ with $U_0 = 0$ and $U_1 = 1$. Then, by induction on $n \geq 2$, it is obtained that $p \nmid U_n$ for all $n \geq 1$ which is a contradiction. Thus, $gcd(n, QD) = 1$. □

Theorem 7: (**Hindi Selfridge-Lucas Test - HLT**) An odd number $n > 11$ is prime if $n | U_{n+1}$ with $n \nmid V_{n+1}$ such that $3^{n-1} \equiv 1 \ (mod \ n)$ by using the Selfridge method for the selection of P and Q.

Proof: Suppose that n is an odd composite number, then n is either Luca's pseudo prime or a Carmichael number. Hence, $n | U_{n+1}$ with $\left(\frac{D}{n}\right) = -1$ and by Selfridge method $P = Q = 0$ whenever $\varepsilon(n) \neq -1$. This proves that n has at least one factor. Thus, from Lemma 1 we obtain that $\gcd(n, 2DQ) = 1$ and n does not satisfy the FLT. Now, define the function $\psi_D(n)$ with $D > 1$ for $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ as follows:

$$\psi_D(n) = \frac{1}{2^{r-1}} \prod_{i=1}^{r} p_i^{\alpha_i - 1} \delta(p_i).$$

So that, $\psi_D(n) = \delta(n)$ and thus n is prime which is a contradiction.

Case 1: if $\alpha > 1$ and $n = p^\alpha$, then $\varepsilon(n) = n$ is not a multiple of p. It follows that, $\psi_D(n) = p^\alpha - p^{\alpha-1} \ \varepsilon(p)$ and note that, $\psi_D(n) \geq n - \ \varepsilon(n) \geq p^\alpha - 1$. But, $p^\alpha - p^{\alpha-1} < p^\alpha - 1$ which implies that $\varepsilon(p) = -1$ and $\delta(n) = p^\alpha \pm 1$ is a factor of $\psi_D(n)$ and this is impossible. Hence, n is prime. On the other hand, we have $Q^{\frac{n-1}{2}} \not\equiv \left(\frac{Q}{n}\right) (mod \ n)$, which implies that $Q^{n-1} \not\equiv 1 \ (mod \ n)$ because $\left(\frac{D}{n}\right) = -1$ and $gcd(n, 2QD) = 1$. Now, by using the algebraic fact that $V_{n+1}^2 = DU_{n+1}^2 + 4Q^{n+1}$ and if n is a factor of U_{n+1}, which implies that $V_{n+1}^2 \equiv 4Q^{n+1} (mod \ n) \not\equiv 2Q^2 (mod \ n)$. Thus, n must be prime.

Case 2: if $r > 1$, then $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ and $\psi_D(n) \leq 2n \prod_{i=1}^{r} \frac{1}{2}\left(1 + \frac{1}{p_i}\right) < n - 1 \leq \delta(n)$ as $n > 11$, which contradicts the hypothesis. Hence n must be prime.

□

For example, if $n = 35207$ with applying Selfridge method and selecting $D = 1$, and $\{P, Q\} = \{1, -1\}$, then $U_{35208} \equiv 0 \ (mod \ 35207)$ and $3^{35207-1} \not\equiv 1 \ (mod \ 35207)$. Hence, it is obtained by **HLT** that n is a composite number. On the other hand, if $n = 1829$, then by applying Selfridge method and selecting $D = -15$ and $\{P, Q\} = \{1, 4\}$, as such the sequences $U = \{1, \ 33, \ 33, \ 33, \ 470, \ 470, \ 470, \ 449, \ 865\} \ (mod \ 1829)$ and $V = \{1822, \ 1882, \ 1882, \ 1882, \ 1265, \ 1265, \ 1265, \ 1370, \ 533, \ 901\} \ (mod \ 1829)$ are obtained.

Hence, $n = 1829$ is a Lucas pseudoprime. But, $3^{1829-1} \not\equiv 1\ (mod\ 1829)$ which implies that $n = 1829$ is not prime.

Remark 1: The overall time complexity of the **HLT** approach is twice the time needed for the computation of $a^n (mod\ m)$. So, by using matrix representation [11, 12], it is acquired that the time complexity is of order $O(n^4 \log^3 n)$. This result is tested on all numbers until $800{,}000$ digits and none of them satisfies Theorem 7.

Baillie-PSW Primality Testing -PSWT

This test has been presented in 1980 by Baillie, Pomerance, Selfridge, and Wagstaff known as the BPSW or BSW test [13, 14]. The process of this test begins with the trial division test which checks for small prime divisors $p < 1000$, then continues with the Miller-Rabin test and terminates with the Lucas sequence test using either Baillie's method or Selfridge's method for selecting $P, Q,$ and D (see [15]).

The trial division test is an easy test proposed by Fibonacci and its idea is based on the following essential theorem [5].

Theorem 8: (Trial Division Test) A positive integer n is said to be composite if it has a prime divisor $p \leq \sqrt{n}$.

Theorem 9: (**Strong-Lucas Test** [13, 14]) Let n be an odd positive integer, and let $\{U_n\}_{n\geq 0}$ and $\{V_n\}_{n\geq 0}$ be Lucas sequences with $n - \left(\frac{D}{n}\right) = 2^s d$ for $s > 1$ and d is odd. If $U_d \not\equiv 0\ (mod\ n)$ and $V_{2^i d} \not\equiv 0\ (mod\ n)$ for $i = 0, 1, \dots, s\ -\ 1$ with $gcd(n, D) = 1$, then n is not prime.

Lucas pseudoprimes are those odd composite numbers that proceed the test as primes. For example, if $n = 25199$, $D = -7$, and $\{P, Q\} = \{1,2\}$ are chosen by Selfridge's method such that $\left(\frac{-7}{25199}\right) = -1$, then by using successive divisions for $n + 1 = 24 \times 575$, it is obtained that $U_{1575} \equiv 24980 \not\equiv 0\ (mod\ 25199)$ and $V_{2^i 1575} \equiv \{18406, 23869\}\ (mod\ 25199)$. This implies that n is a Lucas prime. However, $25199 = 113 \times 223$ is a Strong-Lucas pseudoprime.

The next deterministic test that is based on the generalization of FLT [16, 17] by using the polynomial extension as shown below as lemma

Lemma 2: If p is an odd number and if $a \in Z$ with $gcd(a,p) = 1$, then p is prime if and only if $(x + a)^p \equiv (x^p + a)\ (mod\ p)$ in $Z[x]$.

Also, the double module notation for polynomial congruency and perfect power number is introduced in the following definitions:

Definition 2: Let K be a ring and let $f(x), g(x), h(x) \in K[x]$ with $n \in N$. Then, $f(x) \equiv g(x)(mod\ \ h(x), n)$ if there exists $P\,(x), Q(x) \in K[x]$ such that $f(x) - g(x) = nP(x) + Q(x)h(x)$.

Definition 3: A positive integer n is called a perfect power of a if $n = a^b$ where a and b are greater than 1.

AKS Primality Test

This method is the newest deterministic polynomial algorithm for primality testing which appeared in 2002 and has been suggested by Agrawal, Kayal, and Saxena [16]. It is based on a generalization for Fermat's Little Theorem [16, 17].

Lemma 3: If p is an odd number if $a \in Z$ with $gcd(a,p) = 1$, then p is prime if and only if $(x + a)^p \equiv (x^p + a)\ (mod\ p)$ in $Z[x]$.

Lemma 3 is not efficient and not practical to use as a primality test due to its huge running time during the evaluation of $(x + a)^n\ (mod\ n)$. To eliminate the polynomials of higher-degree, it is suggested to use the n^{th}-degree cyclotomic monic polynomials. This leads to introducing of the double modulo notation in the polynomial congruency class in $Z_n[x]/(h(x))$ where $h(x)$ is a monic irreducible polynomial.

Definition 2: Let K be a ring and let $f(x), g(x), h(x) \in K[x]$ with $n \in N$. Then, $f(x) \equiv g(x)(mod\ \ h(x), n)$ if there exists $P\,(x), Q(x) \in K[x]$ such that $f(x) - g(x) = nP(x) + Q(x)h(x)$.

Hence, if $f(x) \in Z_n[x]$ is an arbitrary monic polynomial, then $(x + a)^n \equiv (x^n + a)\ (mod\ f(x), n)$ for every integer a which leads to a rapid check if the $deg(f(x))$ is not too large. In the following, denote by $T(a, n, r)(x)\ to\ be\ (x + a)^n - x^n - a \equiv 0\ (mod\ x^r - 1, n)$ with $r \leq n$ and $gcd(r, n) = 1$.

Definition 3: A positive integer n is called the perfect power of a if $n = a^b$ where a and b are greater than 1.

The **AKS** primality test is based on the following theorem found in [17], and its proof can be found in [16].

Theorem 10: (**AKS test**) If n and r are two relatively prime positive integers greater than 1 with $ord_r(n) > \log^2 n$ in Z_r^*, and if $T(a, n, r)(x) \equiv 0\ (mod\ x^r - 1, n)$ holds for all $a \in [0, \sqrt{\phi(r)}\ log\ n]$, then n is prime if and only if n is not a perfect power and has no prime factors in $[1, \sqrt{\phi(r)}\ log\ n]$.

For example, let $n = 2017$, $a \in [0, \log n]$, and $r = 107$ such that $O_r(n) > \log^2 n$. It is easy to verify that n is not a perfect power of x for all $b \in [2, \log^2 n]$ and $x > 1$. In addition, if $a = 5$ then $T(5, 2017, 107)(x) = (x + 5)^{2017} - x^{2017}\ - 5\ \equiv 0\ (mod\ x^{107} - 1, 2017)$ which confirms that 2017 is prime by the **AKS** test. However, if $n = 561$, then $T(7,561,3)(x) = (x+7)^{561} - x^{561} - 7 \not\equiv 0\ (mod\ x^3 - 1, 561)$. Hence, $n = 561$ is not prime.

In addition, the **AKS** team left a conjecture which reduces the number of steps in the computation process [16].

Conjecture 1: If r is a prime number such that $r \nmid n$ and if $T(-1,n,r)(x) \equiv 0\ (mod\ x^r - 1, n)$, then n is either prime or $n^2 \equiv 1\ (mod\ r)$.

Remark 2: If Conjecture 1 is valid, then a small method can be modified for suitable $r \in [2, 4\ log\ n]$ such that $r \nmid n^2 - 1$ and of order $O(r \log^2 n)$ for the congruence computation steps. Thus, the overall complexity is of order $O(\log^3 n)$. In addition, it is obtained that searching for r can be excluded by using the following new conjecture.

Conjecture 2: If t is the number of digits for the positive integer $n > 1$ and if $r = \lfloor \sqrt{t} \rfloor$, then n is considered prime if $T(1,n,3r-1)(x) \equiv 0\ (mod\ x^{3r-1} - 1, n)$.

Analysis of the AKS Test

To analyze the correctness of the AKS algorithm presented and proved in [16], we have to use the following theorem presented in [18].

Theorem 11: AKS algorithm returns "True" if and only if n is prime.

The demonstration of the correctness of the **AKS** algorithm starts by using Theorem 10 by verifying that n is not a proper power. Then, the algorithm is used in order to find r for checking whether n has a factor over the interval $[2, \sqrt{\varphi(r)} \log n]$ or not. If so, then the algorithm reports "False". Otherwise, the last step is performed by checking the binomial congruence that must hold for all a in $[1, \sqrt{\varphi(r)} \log n]$ in case n is prime. The next scenario is about even if Theorem 10 holds for all $a \in [2, \sqrt{\varphi(r)} \log n]$ and whether n has prime factors $p > \sqrt{\varphi(r)} \log n$ or not. Consequently, n must be proper power which is already checked in the first step. If so, n must be prime.

The analysis of this method is continued by selecting a suitable value for r which must be bounded in a polynomial time of order $O(log\ n)$. The proof of the following lemma can be found in [18, 19].

Lemma 4: Let n be a positive odd number. Then, there exists a prime number $r \nmid n$ such that $r \le \lceil 16 \log^5 n \rceil$ and $O_r(n) > 4 \log^2 n$.

In the literature, there are some improvements for the AKS in order to reduce its complexity time by choosing the suitable value of r (see [18]). Lenstra [20] has changed the bound for appropriate r by reducing its bound to $O_r(n) > 4 \log^2 n$. Despite that, the algorithm is still inefficient since its complexity is still exponential. After that, the time complexity for choosing the appropriate r has been reduced by using the following theorem (see Cao [19]).

Theorem 12: (**AKS-Bernstein test** [21]) Assume that q and r are prime numbers such that $q|(r-1)$ and $n^{\frac{r-1}{q}} \notin \{0,1\}\ (mod\ r)$ and $\binom{q+s-1}{s} \ge n^{2\sqrt{n}}$ where $S = \{a, b \in Z | a \neq b\ and\ gcd(n, a-b) = 1\}$ is finite of $|S| = s$ integers. If n has no prime factor less than s and $T(a,n,r) \equiv 0\ (mod\ x^r - 1, n)$ for all $a = 0, 1, \ldots, s - 1$, then n is a perfect prime power.

The above theorem is hypothetically more efficient because the powers for any integer can be obtained using Newton's iterations by solving $a^b - n = 0$ which is achieved in a polynomial time. But, the binomial congruence can be processed in $O(sr \log^2 n)$ steps using the Fourier transformations algorithm. Furthermore, it is obtained that the binomial congruence can be summarized in only two steps with the use of Theorem 12. In the following, a conjecture is exhibited which may enhance the behavior of the **AKS** test.

Conjecture 3: Assume that there exist two positive integers q and r such that q is the largest factor of $r - 1$, and $n^{\frac{r-1}{q}} \not\equiv \{0,1\}(modr)$ with $\binom{q+s-1}{s} \ge n^{2\sqrt{n}}$. If $T(a,n,r)(x) \equiv 0(mod\ x^r - 1, n)$ for $a = 2, 3$, then n is prime.

Primality Testing for Special Numbers

In this part, a discussion of three different primality tests is presented for those numbers of the form $t_n = k2^m + b$ where n, k, b, and $m = 2^n$ are positive integers with $k < 2^m$. These tests are the Lucas-Lehmer test, Proth's test, and the new primality testing for Mersenne numbers (**HAT**).

Remark 3: The above form of t_n gives special numbers by choosing special values for k, b, and m. In particular, if $k = b = 1$, and $m = 2n$, then t_n is a Fermat number F_n. Also, if k is odd and $b = 1$ such that $k < 2^m$, then t_n is a Proth's number P_n. Moreover, if $k = 1$ and $b = -1$, then t_n is a Mersenne number M_n.

Lucas-Lehmer Test for Mersenne Numbers [22]

This test is considered a deterministic primality test for Mersenne numbers. It is based on the recursive Lucas sequence in the special case $\{P, Q\} = \{4,1\}$.

Definition 4: (**Lucas-Lehmer sequence**) Let $\{V_k\}_{k>0}$ be a recursive sequence with $\{P, Q\} = \{4,1\}$ such that $V_0 = 4$ and $V_{k+1} = V_{k^2} - 2$ for $k = 0, 1, \ldots$

Remark 4:[10, 23,] If $\delta = (1 \pm \sqrt{3})/\sqrt{2}$, then $\alpha = \varepsilon^2 = 2 + \sqrt{3}$ and $\beta = \delta^2 = 2 - \sqrt{3}$ with $\varepsilon\delta = -1$, and $\varepsilon + \delta = 2\sqrt{6}$. Hence, $\alpha\beta = 1$ and $\alpha + \beta = 4$. Therefore, $V_k = \alpha^{2^{k-1}} + \beta^{2^{k-1}}$ is true for every $k > 0$, and thus $\{V_k\}_{k>0}$ is a Lucas sequence associated to $\{P, Q\} = \{4,1\}$.

The proof of the following lemma and theorem can be found in [23, 24].

Lemma 5: If $M_n \equiv 7\ (mod\ 24)$ is prime, then $\alpha^{\frac{M\_n+1}{2}} \equiv -1\ (mod\ M_n)$ with $n > 2$.

Theorem 13: (**Lucas-Lehmer Test** – **LLT** [24]) Let $\{V_k\}_{k>0}$ be a Lucas sequence presented in Definition 4, then M_n is prime if and only if $M_n | V_{n-2}$ for $n \geq 2$.

For example, if $n = 31$ with $\{P, Q\} = \{4,1\}$ and $D = 12$, then $V_{29} \equiv 0\ (mod\ M_{31})$. This means that M_{31} is a prime number. However, M_{97} is not prime since $V_{95} \not\equiv 0\ (mod\ M_{97})$.

HAT For Mersenne Numbers

The **HAT** is a novel approach for primality testing of Mersenne numbers. The idea of this test is the same as that of Pepin's primality testing for Fermat numbers.

Theorem 14: (**Pepin's Test** [25]) The Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if $3^{\frac{F_n - 1}{2}} \equiv -1 (mod\ F_n)$.

Conjecture 4: (**HAT**) The Mersenne number $M_n$with $n > 3$ is prime if and only if $3^{M_n - 1} \equiv 1 (mod\ M_n)$.

The sufficient condition is a direct application of Fermat's Little Theorem. However, the necessary condition needs an algebraic construction to be proven. A simulation has been done for around 900,000-digit Mersenne numbers using Mathematica and it has proved to be perfect in its outcomes and output running time compared to the Lucas-Lehmer test.

Example 1: If $n = 17$, then $3^{M_{17} - 1} \equiv 1 (mod\ M_{17})$ which implies that M_{17} is prime. However, if $n = 11$, then $3^{M_{11} - 1} \not\equiv 1\ (\ mod\ M_{11})$ which implies that M_{11} is not prime.

Comparative Study:

This study is based on computing the area under the smooth cubic spline interpolated curve where each $(x_i, f(x_i))$ value is determined. Then, a comparison of the graphs of the curves is done by comparing the areas under the curves to decide the most and the least powerful primality tests. This study is done by selecting random primes in the intervals $I_n = [10^n, 10^{n+1}]$ where $n \in Z^+$. Then, running time (time required for each test) is taken down for each chosen input by using the Mathematica built-in function **AbsoluteTiming[.]**. In addition, the study is divided into three parts according to the natural property and algebraic structure of the primality test under the study. Also, each part is divided into many branches depending on a given scale after changing the size of I_n to be $I_{n,k} = [10^{nk}, 10^{nk+1}]$ for $n \in Z^+$, and k is fixed which is entered by the end user. Finally, the collected data are represented in a graph to point out the results.

Probabilistic Primality Tests

The comparative analysis of this study is based on the computation of norms for smooth functions by determining the area under the curve using cubic splines interpolation. This analysis is considered a good reference because it aims at ordering the smooth curves as well as comparing them. First, a simulation is done using the deterministic algorithms (FT, SST, MRT) with a modification on the base $a = r(mod\ (n-1)) + 1$, where r is a fixed positive integer for both; the SST and the MRT. In addition, new modified tests called the SST* and the MRT* are performed to determine the errors based on the percentage of the pseudoprimes which may show up. This simulation is done on random bases $a \in [2, \beta]$ with $\beta > 10^6$ and by the help of the Mathematica function **PrimePi[.]**.Then the Pseudoprime average for each algorithm is determined and the results are summarized and presented as shown in Fig. 1. This proves that, even if the bases are special, there will be a high percentage of errors in reporting the composite numbers as primes. Moreover, it can be noticed that the MRT is the most powerful algorithm relative to pseudoprimes.

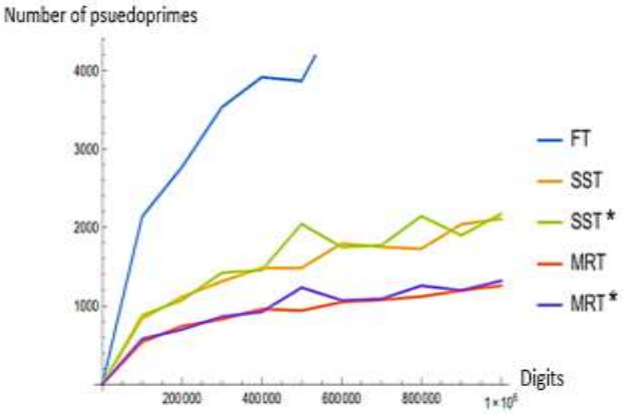


Figure 1. Average number of Pseudoprimes for each primality test from digit 1 to 10^6.

Random Primality Tests

By choosing random primes using the built-in function **PrimeQ[.]** in order to select new primes taking into consideration the number of digits of the input in the interval I_n. The following graph is obtained as shown in Fig. 2:

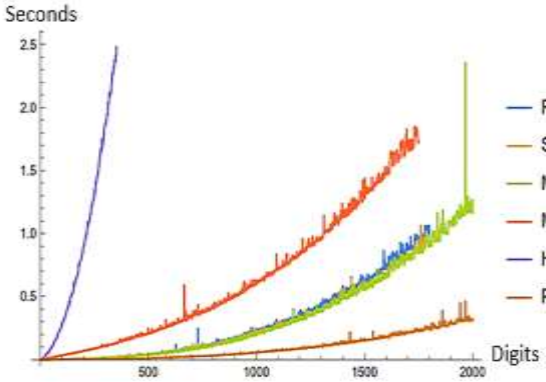


Figure 2. Running time for PSWT, HLBT, MRBT, MRT, SST, and FT. from digit 1 to 2000

It is clear from Fig. 2 that the running time data of the tests are so closed and periodic. Thus, to be more specific, subintervals are used in order to get clear observations and conclusions and obtain the Figs.3- 5:

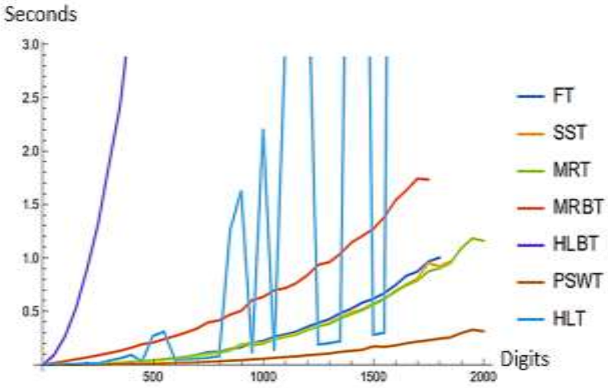


Figure 3. Running time for HLT, PSWT, HLBT, MRBT, MRT, SST, and FT with width 50 for I_n.

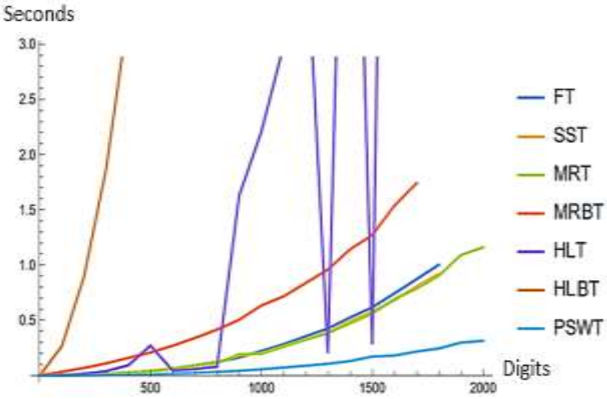


Figure 4. Running time for PSWT, HLBT, HLT, MRBT, MRT, SST, and FT with width 100 for I_n.

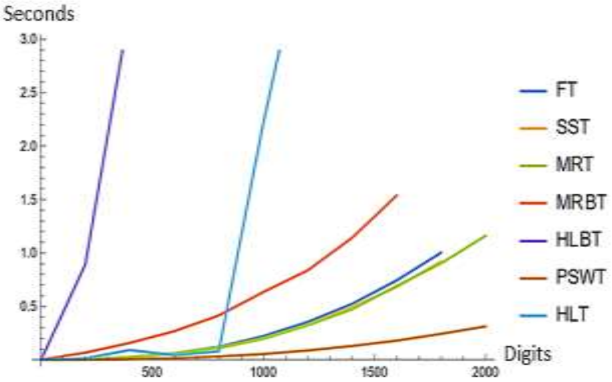


Figure 5. Running time for HLT, PSWT, HLBT, MRBT, MRT, SST, and FT with width 200 for I_n.

Based on Fig. 5, it is noticed that **HLBT** is the least powerful primality test with an exponential shape. However, **PSWT** is the most powerful test with $\log_2 n$ shape. In order to be more precise in arranging the primality tests, the researchers used both L_1 and L_∞ norms. The results are collected in a table after each simulation. Then, the area under the curve is measured by using the L_∞ norm in order to check how much time each primality test takes. This process is repeated for those with the least powerful results. The results obtained show that **HLBT** is the least powerful primality test while the **PSWT** test is the most powerful one during this experiment. Also, **FT** is considered one of the least powerful (slowest) tests, whereas the **MRT** is considered the most powerful (fastest) test in the case of the randomized category algorithm. In addition, to get rid of all the doubts about **HLBT** and **MRT**, L_1 norm is used on continuous subintervals I_n where all the curves have the same endpoints. The results are shown in Fig. 6.

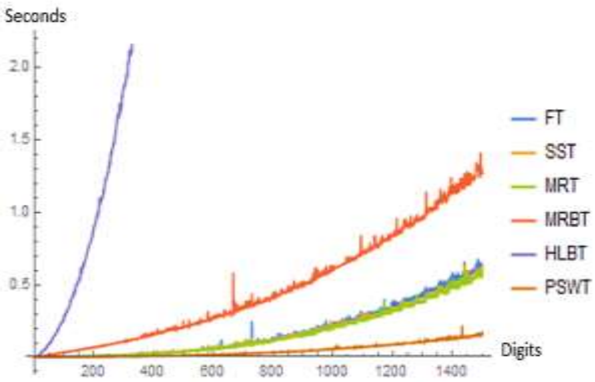


Figure 6. Curves for the cubic spline interpolation of the data points obtained from the PSWT, HLBT, MRBT, MRT, SST, and FT from digit 1 to 1500.

Although the numerical approach of the L_1 is so exhausting and uncertain for the computer to give outputs when the table consists of more than

1400 rows, it is considered more accurate than other norms. So, the next observations are used for the tests according to the L_1 norm up to 2000 digits and the results are shown in Figs. 7 and 8.

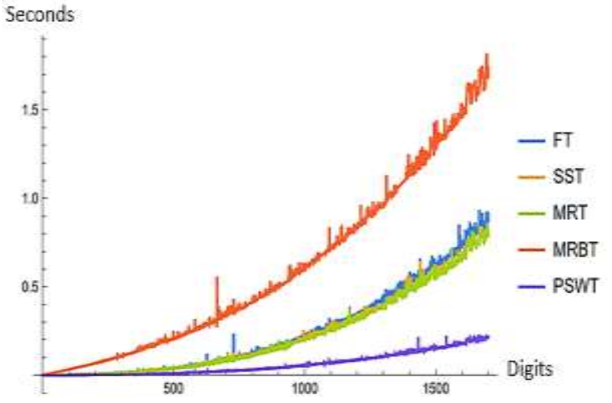


Figure 7. Curves for the cubic spline interpolation of the data points obtained from the PSWT, MRBT, MRT, SST, and FT from digit 1 to 1750.

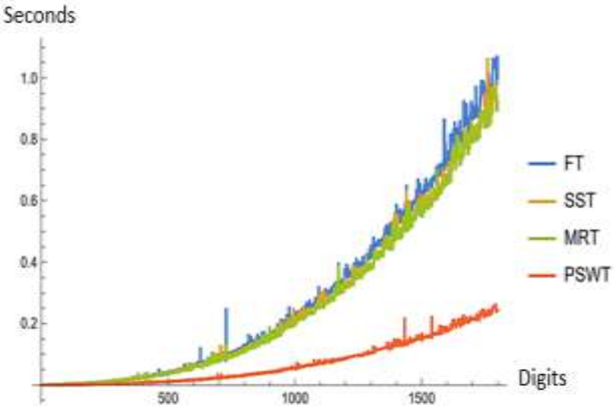


Figure 8. Curves for the cubic spline interpolation of the data points obtained from the PSWT, MRT, SST, and FT from digit 1 to 1800.

Now, by skipping the algorithms that reach the maximal limited running time, it can be obtained from Figs. 6 and 7 that **MBRT** and **HLBT** should be canceled from the study.

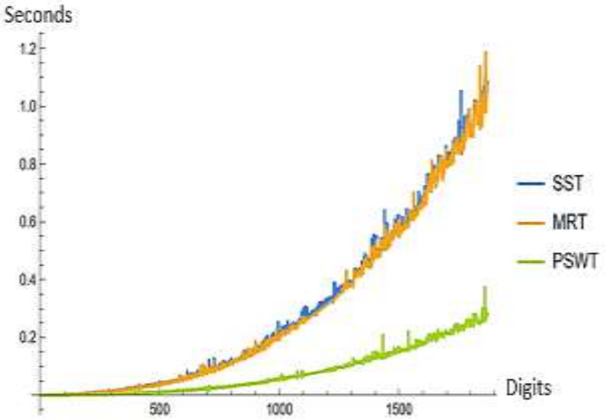


Figure 9. Curves for the cubic spline interpolation of the data points obtained from the PSWT, MRT, and SST from digit 1 to 1870.

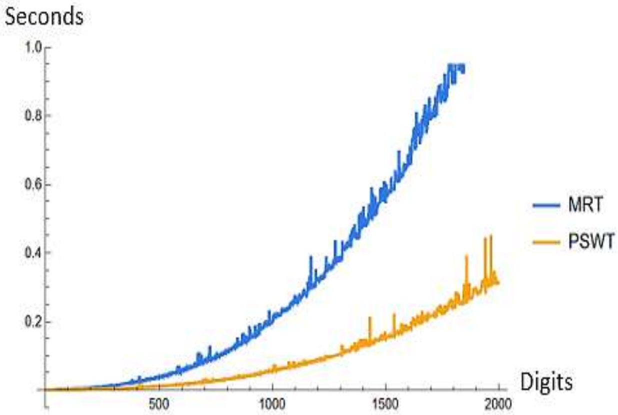


Figure 10. Curves for the cubic spline interpolation of the data points obtained from the PSWT and MRT from digit 1 to 2000.

Now, it is obvious from Figs. 9, 10 that **SST** and **MRT** approximately have the same running time, and the difference between their areas under the curve is approximately $10.0143\, u^2$. Hence, it is obtained that **MRT** is better than **SST** according to its accuracy, smoothness, and rapidness. In addition, it can be observed that **PSWT** is the most powerful primality test, yet **SST** and **MRT** are so not accurate and can be considered the least powerful primality tests in doing their task. To be more specific and accurate, the same study is repeated but with different fixed variable k which is added after observing that the computations of the L_1 norms are demanding and exhausting to the computer which yields using new subintervals $I_{n,k}$. In this way, the speeding up of the experiment becomes more powerful in investigating and testing new primes. Moreover, the shape of the timing curve becomes clearer and smoother. The analysis starts by taking $k = 100$ and the endpoint of the interval is 10000.

In addition, in Table 1, the L_∞ norm is used in 7 rounds, where in each round the least powerful test is skipped from the list and a new round is done with the remaining tests. Then, in the new round, the least powerful from the new list of tests are skipped from the list, and so on. After seven successive rounds, the tests are arranged from the least powerful test to the most powerful one. In addition, the frequency of each curve in each round is computed by using the formula $\% = \frac{\max frequency}{Total \max frequency\ for\ all\ case} \times 100$, and the test of the least frequency in such round is skipped in the second round, and so on.

Table 1. Norm max from digit 1 to 10000 with the length size I_n equals 100.

Type	Round 1	Round 2	Round 3	Round 4	Round 5	Round 6	Round 7
FT	3	29	39	22	8	0	0
SST	0	4	24	40	31	2	0
MRT	1	3	14	36	27	20	0
MRBT	31	46	21	3	0	0	0
HLT	28	17	3	0	35	18	0
HLBT	38	2	0	0	0	0	0
PSWT	0	0	0	0	0	61	40
Total	101	101	101	101	101	101	40
Max	38	46	39	40	35	20	40
%	HLBT 17.4311	MRBT 21.1009	FT 17.8899	SST 18.3486	HLT 16.0550	MRT 9.17431	PSWT

FT: Fermat test; SST: Solovay-Strassen Test; MRT: Miller-Rabin test; MRBT: Miller Rabin test with binary representation for n; HLT: Hindi Lucas Sequenced test; HLBT: Hindi Lucas sequence with binary representation for n test; PSWT: Baillie–PSW primality test.

Based on Table 1, it can be claimed that **HLBT** is the least powerful primality test however **PSWT** is the most powerful one. Moreover, if computations of L_1 are continued for the other primality tests, Fig. 11 is obtained.

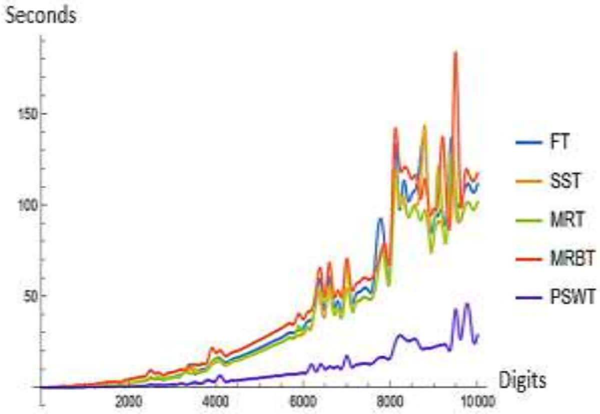


Figure 11. Curves for the cubic spline interpolation of the data points obtained from the PSWT, MRBT, MRT, SST, and FT from digit 1 to 10000.

To sum up, the first part of this analysis is done when $k = 100$, and from Fig. 11, it can be declared that **PSWT** is the most powerful and effective algorithm for primality testing, while **MRBT** and **FT** are the least powerful and exhausting algorithms since they consume lots of time. In addition, even if the binary representation for n as the method is used, it is no longer helpful and effective for **HLBT** and **MRBT**.

Now, if $k = 5000$ with an interval endpoint which is 20000 is taken, then Fig. 12 is obtained.

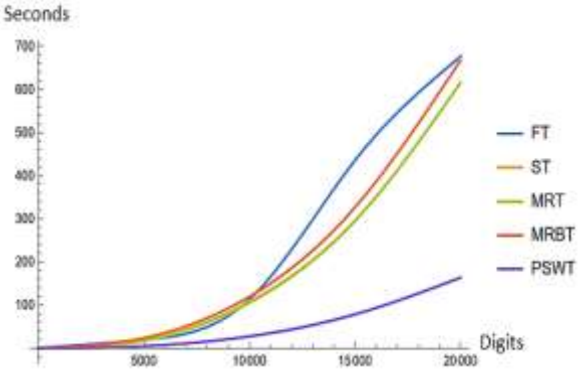
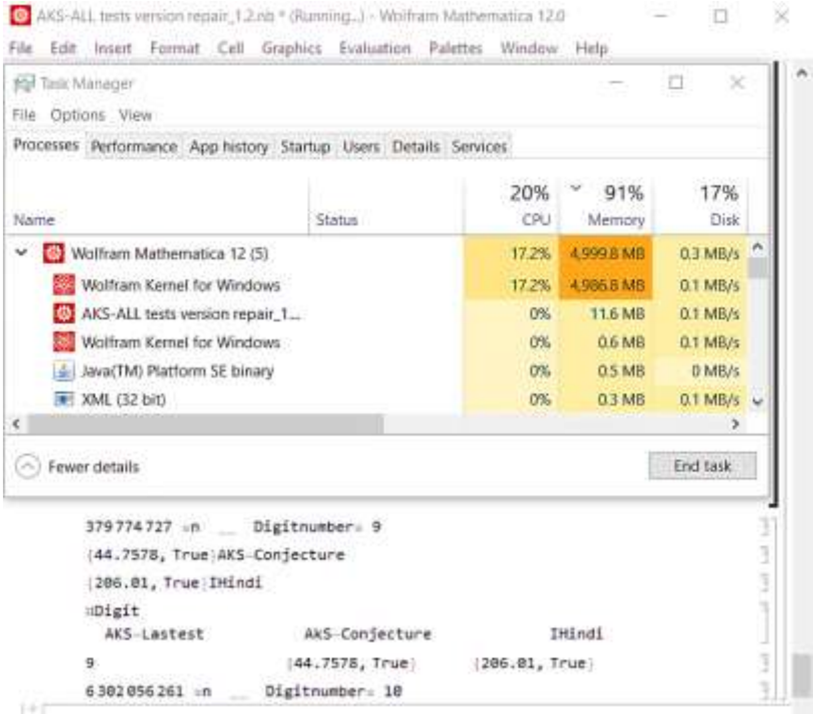


Figure 12. Curves for the cubic spline interpolation of the data points obtained from the PSWT, MRBT, MRT, SST, and FT from digit 1 to 20000.

From the results which have been obtained in Figs.11 and 12, it can also be declared that **FT** is the least powerful primality test and **PSWT** is the most powerful one. Moreover, **MRT** dominates **SST** in the different area $13464.8\, u^2$. Finally, it can be deduced that **PSWT** is the most reliable, and straightforward primality test, while **HLT** and **HLBT** are the least reliable and demanding primality tests.

AKS Primality Test

The AKS primality test is removed from this study because of the following reasons: First, technically it requires a large space in the memory of the computer during the computation process which is of polynomial congruency [1]. Second, there are insufficient improvements for reducing the demanding iterations for the computer speed and memory. Finally, its curve is unclear compared with the curves of the other primality tests such as FT, SST, MRT, and PSWT (see Fig. 13).


AKS-ALL tests version repair_1.2.nb * (Running...) - Wolfram Mathematica 12.0
File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

Name	Status	20% CPU	91% Memory	17% Disk
Wolfram Mathematica 12 (5)		17.2%	4,999.8 MB	0.3 MB/s
Wolfram Kernel for Windows		17.2%	4,986.8 MB	0.1 MB/s
AKS-ALL tests version repair_1...		0%	11.6 MB	0.1 MB/s
Wolfram Kernel for Windows		0%	0.6 MB	0.1 MB/s
Java(TM) Platform SE binary		0%	0.5 MB	0 MB/s
XML (32 bit)		0%	0.3 MB	0.1 MB/s

```
379 774 727 =n    Digitnumber= 9
{44.7578, True}AKS-Conjecture
{206.01, True}IHindi
=Digit
  AKS-Lastest          AKS-Conjecture          IHindi
9                    {44.7578, True}      {206.01, True}
6 302 056 261 =n    Digitnumber= 10
```

Figure 13. Evidence of painful loops on the computer.

Mersenne Primality Tests

In the following section, a study for Mersenne primality tests is done. In fact, a survey about which primality test is the most reliable in hunting Mersenne primes is performed. So, all the primality tests in this study are processed in order to hunt the Mersenne numbers less than 895932. In Table 2, the L_∞ norm is used as in Table. 1 but it took nine successive rounds to arrange them from the least powerful test to the most powerful one.

Table 2. Norm infinity from digit 1 to 895932.

Type	Round 1	Round 2	Round 2	Round 3	Round 4	Round 5	Round 6	Round 7	Round 9
LLT	1	0	1	1	3	2	10	13	3
HAT	0	1	0	1	1	2	1	10	18
FT	0	6	11	2	1	6	3	0	0
SST	2	2	4	15	9	0	0	0	0
MRT	1	2	3	9	14	3	0	0	0
MRBT	6	17	3	2	1	0	0	0	0
HLT	1	0	8	3	2	16	3	0	0
HLBT	23	5	0	0	0	0	0	0	0
PSWT	0	1	3	0	1	3	12	6	7
Total	34	34	33	33	32	32	29	29	28
Max	23	17	11	15	14	16	12	13	18
Test	HLBT	MRBT	FT	SST	MRT	HLT	PSWT	LLT	HAT
%	19.0082	14.0495	9.0909	12.3966	11.5702	13.2231	9.9173	10.7438	0

LLT: Lucas Lehmer test; HAT: Hindi Awad test; FT: Fermat test; SST: Solovay-Strassen Test; MRT: Miller-Rabin test; MRBT: Miller Rabin test with binary representation for n; HLT: Hindi Lucas Sequenced test; HLBT: Hindi Lucas sequence with binary representation for n test; PSWT: Baillie–PSW primality test.

From the results in Table. 2, it can be observed that the least powerful algorithm in hunting Mersenne primes is **HLBT**, whereas the most powerful one is **HAT**. So, the study is focused only on **PSWT**, **LLT**, and **HAT**. It may be inferred that **HAT** (new approach) is the most reliable primality test for Mersenne primes. In addition, the L_1 norm test is used for more accuracy, and the results are shown in Fig. 14.

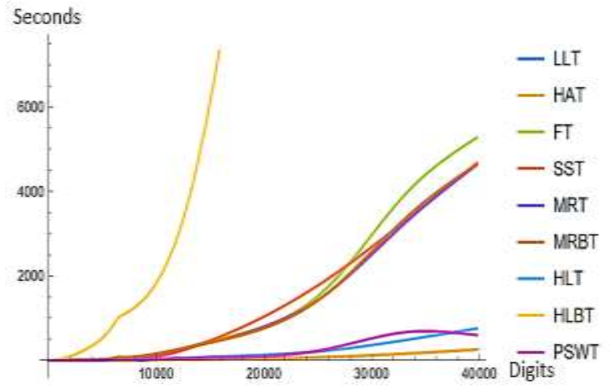


Figure 14. Curves for the cubic spline interpolation of the data points obtained from the PSWT, HLBT, HLT, MRBT, MRT, SST, FT, HAT, and LLT from digits 1 to 39750.

From the results in Fig. 14, HLBT certainly has the largest area compared with the areas of other tests, and as such **HLBT**, **FT**, and **SST** are not the good least powerful tests for Mersenne primes. However, **LLT** and **HAT** are the more reliable ones. Now, if the width of the interval is extended to 420921, it is obtained that **PSWT** is a powerless test and consumes lots of time compared with **HAT** and **LLT**, whereas **HAT** is the most powerful one in this interval. Based on the mentioned observation, **PSWT** and **HLT** are not reliable, deficient, and affect negatively the study. So, these tests are skipped from the study, and the results are shown in Figs.15- 17.

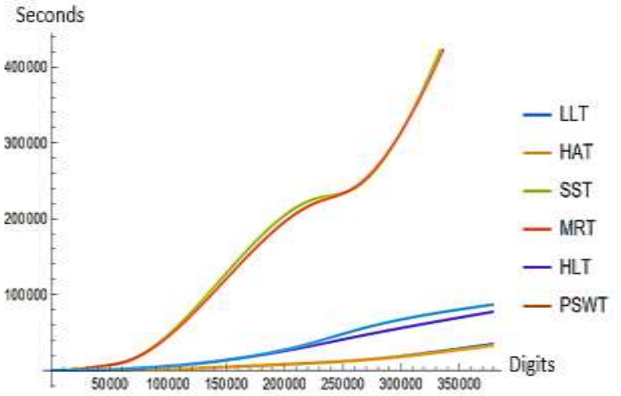


Figure 15. Cubic Spline for LLT, HAT, SST, MRT, HLT, and PSWT from digit 1 to 420921.

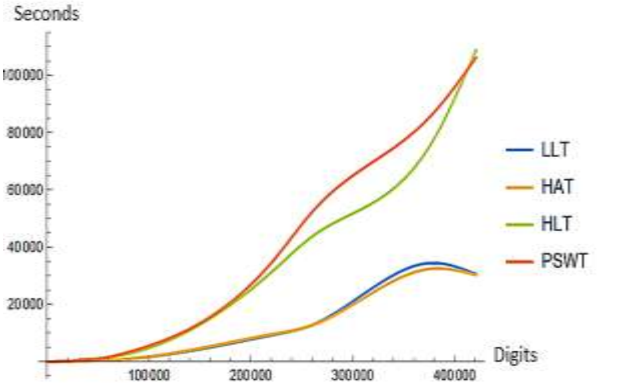


Figure 16. Curves for the cubic spline interpolation of the data points obtained from the PSWT, HLT, HAT, and LLT from digit 1 to 420921.

The experiment continues normally and smoothly for more than two weeks without stopping after digit 895932 until a termination in the program occurs without any noticed output.

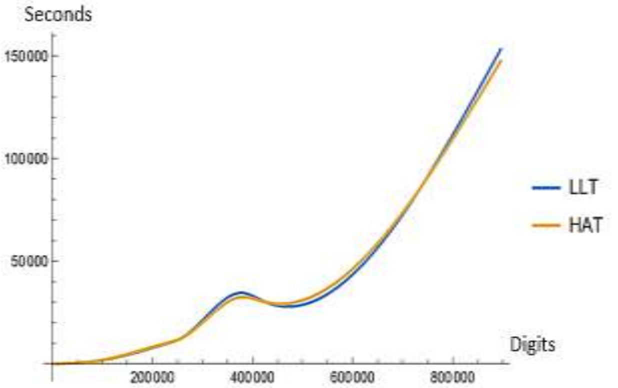


Figure 17. Cubic spline for HAT and LLT from digit 1 to 895932

In addition, from Fig. 17, it is clear that **LLT** exceeds **HAT** by an area equal to $1.90468 \times 10^{7}\ u^{2}$. Hence, it can be declared that **LLT** and **HAT** are the most powerful Mersenne primality tests.

Proth's Primality Test

In this part, Proth's primality test is studied to find Proth's prime numbers $n = k2^{n} + 1$, where $k = \sum_{i=19}^{n} 2i$. As done in Tables 1, and 2, the L_{∞} norm is used in nine successive rounds to arrange the tests from the least powerful test to the most powerful one. The results are presented in Table. 3, and Figs.18- 20 are shown below.

Table 3. Norm infinity from digit 1 to 32907.

Type	Round 1	Round 2	Round 3	Round 4	Round 5	Round 6	Round 7	Round 8	Round 9
PT	0	1	0	0	1	2	8	13	10
PGT	0	11	9	6	1	0	0	0	0
FT	0	3	3	3	7	6	4	9	0
SST	0	0	2	5	9	15	4	0	0
MRT	0	1	9	20	2	3	0	0	0
MRBT	11	13	10	0	0	1	0	0	0
HLT	0	0	0	1	14	4	11	5	0
HLBT	24	6	2	0	0	0	1	0	0
PSWT	0	0	0	0	1	4	7	6	17
Total	35	35	35	35	35	35	35	33	27
Max	24	13	9	20	14	15	11	13	17
Test	HLBT	MRBT	PGT	MRT	HLT	SST	FT	PT	PSWT
%	20.16806	10.9244	7.5630	16.8067	11.7647	12.6050	9.2437	10.9244	0

PT: Proth's test; PGT: Proth's general test; FT: Fermat test; SST: Solovay-Strassen Test; MRT: Miller-Rabin test; MRBT: Miller Rabin test with binary representation for n; HLT: Hindi Lucas Sequenced test; HLBT: Hindi Lucas sequence with binary representation for n test; PSWT: Baillie–PSW primality test.

From Table 3 it can be obtained that **HLBT** is the least powerful primality test, while **PT** and **PSWT** are the most powerful primality tests. To be more precise, the L_1 norm is used to arrange the mentioned primality tests from the least to the most powerful tests. The obtained results are presented in Figs.18-20.

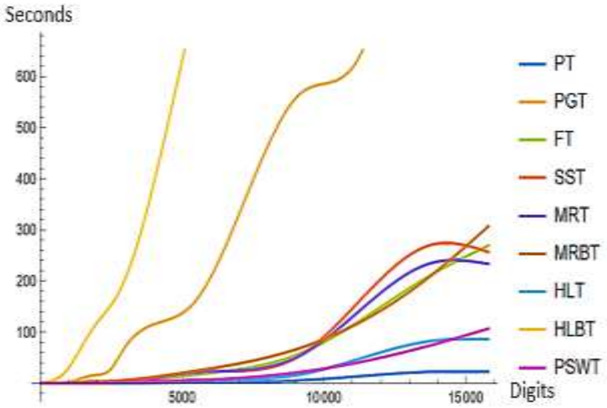


Figure 18. Curves for the cubic spline interpolations of the data points obtained from the PSWT, HLBT, HLT, MRBT, MRT, SST, FT, PGT, and PT from digits 1 to 15811.

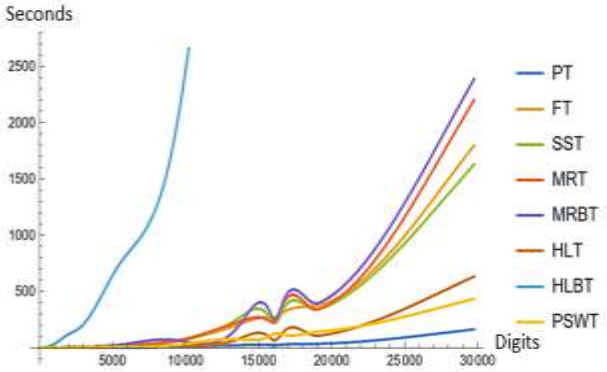


Figure 19. Curves for the cubic spline interpolation of the data points obtained from the PSWT, HLBT, HLT, MRBT, MRT, SST, FT, and PT from digit 1 to 29754.

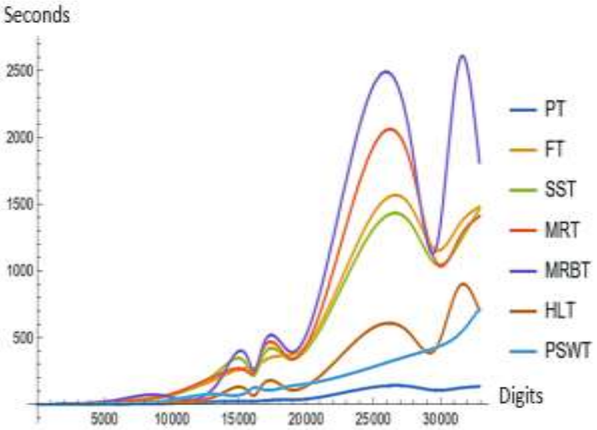


Figure 20. Curves for the cubic spline interpolation of the data points obtained from the PSWT, HLT, MRBT, MRT, SST, FT, and PT from digits 1 to 32907.

From Figs. 18- 20, it can be observed that **HLBT**, **PGT**, and **MRBT** are the least powerful Proth's primality tests, while **PSWT** exceeds **PT** by an area equal to $3.76154 \times 10^6\ u^2$.

Therefore, **PSWT** is the most powerful and reliable primality test for any number.

Conclusion:

Throughout this study, it is proved numerically that **PSWT** is the most powerful and reliable primality test on any number. Moreover, **MRT** is the least powerful and unreliable primality test algorithm in the randomized algorithms for any input. In conclusion, it is declared that **LLT**, **HAT**, and **PT** are the most powerful and reliable primality tests depending on specific inputs. However, it cannot be predicted what will happen for **LLT** and **HAT** if the interval is extended to the largest discovered Mersenne primes.

Acknowledgment:

The authors gratefully thank the Referee for the constructive comments and recommendations which help to improve the readability and quality of the paper.

Authors' Declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Besides, the Figures and images, which are not ours, have been given permission for re-publication and attached to the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at Lebanese International University.

Authors' Contributions Statement:

Y A and R H participated in the development of the idea and the theory of the research. R H, contributed to developing the topic, implementing the Mathematica programs for the comparison study, and collecting the data and graphs. Y A, R H, and H C, engaged in the analysis of the results by writing, revising, proofreading, and discussing the final version of the manuscript.

References:

1. Al-Bundi SS. On Subliminal Cryptography. Baghdad Sci J. 2006; 3(1): 124-130.
2. Khudhair ZN, Nidhal A, El Abbadi NK. Text Multilevel Encryption Using New Key Exchange Protocol. Baghdad Sci J. 2022; 19(3): 0619-0619. https://doi.org/10.21123/bsj.2022.19.3.0619
3. Albrecht MR, Massimo J, Paterson KG, Somorovsky J. Prime and Prejudice: Primality Testing Under Adversarial Conditions. Proc ACM SIGSAC Conf Comput Commun Secur. (CCS'18). 2018: 281-298. https://doi.org/10.1145/3243734.3243787
4. Bunder M, Nitaj A, Susilo W, Tonien J. A Generalized Attack on RSA Type Cryptosystems. Theor Comput Sci. 2017; 704: 74-81. https://doi.org/10.1016/j.tcs.2017.09.009
5. Menezes AJ, Kenneth HR, Van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. Boca Raton: CRC press; 2020. 810 p. https://doi.org/10.1201/9780429466335
6. Banerjee K, Mandal SN, Das SK. A Comparative Study of Different Techniques for Prime Testing in Implementation of RSA. Am J Adv Comput. 2020; 1(1): 1-7. https://doi.org/10.15864/ajac.1102
7. Landau E. Elementary Number Theory. USA: American Mathematical Society; 2021. 256 p.
8. Alqaydi L, Yeun CY, Damiani E. A Modern Solution for Identifying, Monitoring, and Selecting Configurations for SSL/TLS Deployment. Int Conf Appl Comput Inf Technol (ACIT 2018). Springer, Cham. 2018; 78-88. https://doi.org/10.1007/978-3-319-98370-7_7
9. Ramzy A A. Primality Test for Kpn + 1 Numbers and A Generalization of Safe Primes and Sophie Germain Primes. arXiv preprint arXiv: 2207.12407. 2022 Jul 25. https://doi.org/10.48550/arXiv.2207.12407
10. Zheng Z. Prime Test. Modern Cryptography. 2022; 1: 197-228. https://doi.org/10.1007/978-981-19-0920-7_5
11. Andrica D, Bagdasar O. On Generalized Lucas Pseudoprimality of Level k. Mathematics. 2021 Apr 12; 9(8): 838. https://doi.org/10.3390/math9080838
12. Andrica D, Bagdasar O. Pseudoprimality Related to the Generalized Lucas Sequences. Math Comput Simul. 2022; 201: 528-542. https://doi.org/10.1016/j.matcom.2021.03.003
13. Baillie R, Wagstaff SS. Lucas Pseudoprimes. Math Comput. October 1980; 35(152): 1391-1417. https://doi.org/10.2307/2006406
14. Baillie R, Fiori A, Wagstaff Jr S. Strengthening the Baillie-PSW Primality Test. Math Comput. 2021; 90(330): 1931-1955. https://doi.org/10.1090/mcom/3616
15. Crandall R, Pomerance CB. Prime Numbers: a Computational Perspective. Math Gaz. 2002; 86(507): 552-554. https://doi.org/10.2307/3621190
16. Agrawal M, Kayal N, Saxena N. Errata: PRIMES is in P. Ann Math. 2019; 189(1): 317-318. https://doi.org/10.4007/annals. 2019.189.1.6
17. Menon V. Deterministic Primality Testing-Understanding the AKS Algorithm. arXiv preprint arXiv:1311.3785. 2013. https://doi.org/10.48550/arXiv.1311.3785
18. Sridharan S, Balakrishnan R. Discrete Mathematics: Graph Algorithms, Algebraic Structures, Coding Theory, and Cryptography. 1st Ed. New York: Chapman and Hall/CRC Press; 2019. 340 p. https://doi.org/10.1201/9780429486326
19. Cao Z, Liu L. Remarks on AKS Primality Testing Algorithm and A Flaw in the Definition of P. arXiv preprint arXiv:1402.0146. 2014 Feb 2. https://doi.org/10.48550/arXiv.1402.0146
20. Lenstra Jr HW, Pomerance CB. Primality Testing with Gaussian Periods. J Eur Math Soc. 2019; 21(4): 1229-1269. https://doi.org/10.4171/JEMS/861
21. Bisson G, Ballet S, Bouw I. Arithmetic, Geometry, Cryptography and Coding Theory. Amer Math Soc. 2021; 770: 104-131. https://doi.org/10.1090/conm/770
22. Wu L, Cai HJ, Gong Z. The Integer Factorization Algorithm with Pisano Period. IEEE Access. 2019; 7: 167250-167259. https://doi.org/10.1109/ACCESS.2019.2953755
23. Bruce JW. A really trivial proof of the Lucas-Lehmer Primality Test. Am Math Mon. 1993; 100(4): 370-371. https://doi.org/10.1080/00029890.1993.11990414
24. Théry L, Antipolis S. Primality Tests and Prime Certificate. arXiv preprint arXiv: 2203. 16341. 2022. https://doi.org/10.48550/arXiv.2203.16341
25. Kundu S, Mazumder S. Number Theory and its Applications. 1st Ed. London: CRC Press; 2022. 366 p. https://doi.org/10.1201/9781003275947

دراسة مقارنة بين إختبار حتمي جديد لأعداد مرسين الأولية وإختبارات أَوَليَّةِ العددِ المتداولة

يحيا عواض[1] رامز الهندي[1] هيسم شحاده[2,3]

[1] قسم الرياضيات والفيزياء، كلية الآداب والعلوم، الجامعة اللبنانية الدولية، البقاع، لبنان.
[2] قسم الرياضيات والفيزياء، كلية الآداب والعلوم، الجامعة اللبنانية الدولية، صيدا، لبنان.
[3] قسم الرياضيات والفيزياء، كلية الآداب والعلوم، جامعة بيروت الدولية، بيروت، لبنان.

الخلاصة:

في هذا البحث، نقدم اختبار أَوَليَّةِ العددِ جديد لأعداد مرسين (Mersenne numbers $2^n - 1$) تحت إسم إختبار هندي-عواض (HAT). تقوم فكرة هذا الإختبار الجديد على فكرة مشابهه لتلك التي إعتمدت في إختبار بيبين (Pepin's test) لأعداد فيرمات (Fermat numbers $2^{2^n} + 1$). علاوة على ذلك يتضمن هذا البحثُ إقتراح تعديل جديد لمعالجة مكامن الضعف في إختبار سلفريدج و لوكاس (SLT) لأَوَليَّةِ العددِ من اجل التخلص من الاعداد الاولية الكاذبة عبر إقتراح إختبار معدل جديد بعنوان هندي سلفريدج و لوكاس (HLT) بمساعدة ال base 3. وفي الختام، تم تقديم دراسة لمقارنةً إختبارات أَوَليَّةِ العددِ المعروفة والإختبار الجديد من أجل تحديد الأفضلِ بينهم ان كان من حيث مستوى القوة، السرعة، والفاعلية وذلك بناءً على النتائج التي حصلنا عليها عبر برامج تم إعدادها وتشغيلها بواسطة برنامج Mathematica. هذه النتائج تم عرضها في الدراسة عبر جداول ورسومات بيانية.

الكلمات المفتاحية: إختبار حتمي، أعداد ميرسين، إختبار أَوَليَّةِ العدد، إختبار إحتمالي، أعداد بروث.