A Novel Deterministic Mersenne Prime Numbers Test: Aouessare-El Haddouchi-Essaaidi Primality Test

Abdelilah Aouessare
Abdelmalek Essaadi University,
Faculty of Science, Tetuan,
Morocco

Abdeslam El Haddouchi
Abdelmalek Essaadi University,
Faculty of Science, Tetuan,
Morocco

Mohamed Essaaidi
Mohammed V University,
National Higher School of IT,
Rabat, Morocco

ABSTRACT
There has been an increasing interest in prime numbers during the past three decades since the introduction of public-key cryptography owing to the large spread of internet and electronic banking. The largest prime number discovered so far, which is a Mersenne number, has 17,425,170 digits. However, the algorithmic complexity of Mersenne primes test is computationally very expensive. The best method presently known for Mersenne numbers primality testing is Lucas–Lehmer primality test. This paper presents a novel primality test for these numbers, namely, Aouessare-El Haddouchi-Essaaidi primality test, which largely outperforms Lucas-Lehmer test with its very low algorithmic complexity which allows performing much quicker tests with the other advantage of considerable memory requirements savings. Moreover, in the case of a composite number, where this test is negative, it is also possible to decompose the tested number into two factors whose product yields it. It is anticipated that this primality test will be a real progress in the theory of prime numbers and in the conquest of very large prime numbers with the subsequent implication on information security and assurance. Furthermore, this test will also allow factoring very large composite numbers in a very efficient way.

General Terms
The approach presented in this paper is relevant to number theory, and more specifically to prime numbers theory. This theory is strongly related to information cryptography and, thus, to information security assurance and privacy.

Keywords
Prime numbers, Mersennes prmes, primality test, cryptography, security and privacy.

1. INTRODUCTION
Prime numbers are very important for both number theory and mathematics as a whole. They are also particularly important for data encryption which is the essential foundation of information security and security assurance in different technologies such as the internet and electronic banking [1,2].

The search for a good primality test is one of the most important problems of numbers theory and it is by no means a new one. Actually, this is probably one of the very old mathematics problems that goes back to around 2500 B.C. when the ancient priests of Uruk used to engrave long lists of prime numbers in cuneiforms [3].

It is of great interest to investigate prime numbers properties. It is especially interesting to look at those properties which can efficiently determine if a number is prime or not. Those properties are very useful in practice to define large prime numbers for cryptographic protocols used in information security. Many of the largest known primes are Mersenne primes since they are the easiest type of number to prove prime thanks to the Lucas-Lehmer test [4, 5]. They are named after the French monk Marin Mersenne who introduced them in the early 17th century [6].

A Mersenne prime is a prime number is of the form $M_p=2^p-1$, where p is a prime number. The first four Mersenne primes are 3, 7, 31 and 127 for p = 2, 3, 5 and 7, respectively.

The most recent Mersenne prime, the 48th in the list of these numbers, was verified on January 25th, 2013. This is the largest known prime number (i.e. $2^{57,885,161} - 1$) which has 17,425,170 digits [7,8]! Since 1997, all newly found Mersenne primes have been discovered by the "Great Internet Mersenne Prime Search" (GIMPS), a distributed computing project on the Internet. GIMPS has been very successful in expanding the range of prime numbers to unprecedented levels as can be seen in Figure 1.

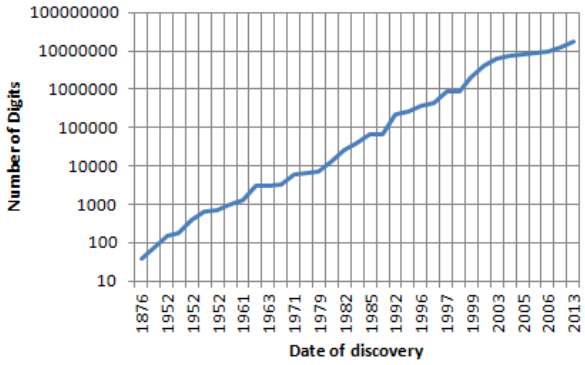

Fig 1 : Number of digits of largest prime number date of discobvery.

The best method so far known and widely used for testing the primality of Mersenne numbers is Lucas–Lehmer primality test. It has been used by the Great Internet Mersenne Prime Search for its quest for very large primes and which has been very successful in identifying many of the largest primes known to date [9].

LUCAS-LEHMER VS PROPOSED PRIMALITY TEST

Lucas_Lehmer test states that for a prime number $p > 2$, $M_p = 2^p - 1$ is prime if and only if M_p divides $S_p - 2$, where $S_p = S_{p-1}^2 - 2$ and $S_0 = 4$.

The algorithmic complexity of this test is O(n2 log n log log n).

The proposed primality test for Mersenne numbers is based on the following theorem.

Theorem 1: Aouessare-El Haddouchi-Essaaidi Primality Test.

Let M_p be a Mersenne prime number (i.e. p is necessarily a prime number such that p>2) and n an integer number such that n>0. Let K_n be the composition number such that

$$K_n = \frac{M_p - (2\,p\,n+1)^2}{6\,p\,(2\,p\,n+1)} \qquad (1)$$

If K_n is a negative real number M_p is a Mersenne prime number, and if it is a positive integer then M_p is a composite number.

In the case of composite number, it is also possible to decompose it according to two factors as outlined by theorem 2 below.

Theorem 2: In the case where M_p is a composite number, it can be written as follows:

$$M_p = (2p\,n + 1)\,(2p\,n + 1 + 6p\,Kn) \qquad (2)$$

A simple inspection of the expression of the composition number K_n, given in theorem 1, shows that the algorithmic complexity of this test is O(n) which is much lower than that of Lucas-Lehmer (i.e. O(n2 log n log log n)).. This fact indicates that it will require much lower number of computations compared with Lucas-Lehmer primality test and therefore, it will be faster in testing numbers in the search of Mersenne primes.

2. RESULTS AND DISCUSSIONS

In order to illustrate these theorems and to show how they work in testing Mersenne numbers and in decomposing composite numbers few examples are given below.

2.1. Example 1: Composite numbers

i. For p = 11, which is a prime number, the corresponding Mersenne number is M_{11} = 2047.

It can be easily verified that K_1 = 1 (obtained for n=1), which means that M_{11} is a composite number. Theorem 2 giving the factors of composite numbers outlined above yields:

M_{11} = 23 x 89.

ii. For p = 29, which is also a prime number, the corresponding Mersenne Number is

M_{29} = 536,870,911.

It can be verified that for n = 4, K_4 = 13,241 (i.e. positive integer number), which means that M_{29} is also a composite number which can be also expressed as a product of two factors according to Theorem 2, namely,

M_{29} = 233 x 2,304,167.

2.2 Example 2: Mersenne prime numbers

Let's consider two examples of Mersenne prime numbers corresponding to p = 7 and 13 which are prime numbers. These Mersenne numbers are M_7 = 127 and M_{13} = 8,191, respectively.

. **Table 1. Aouessare-El Haddouchi-Essaaidi Test.**

M_7	**n**	1			
	K_n	- 0.16			
M_{13}	**n**	1	2	3	4
	K_n	3.54	1.30	0.31	- 0.34

It can be concluded from Table 1 that both numbers M_7 and M_{13} are Mersenne prime numbers since K is negative, as required by Theorem 1, for n = 1 for the first number and for n = 4 for the second one.

From the above examples, it can be seen that the proposed primality test is very efficient in proving the primality of Mersenne numbers.

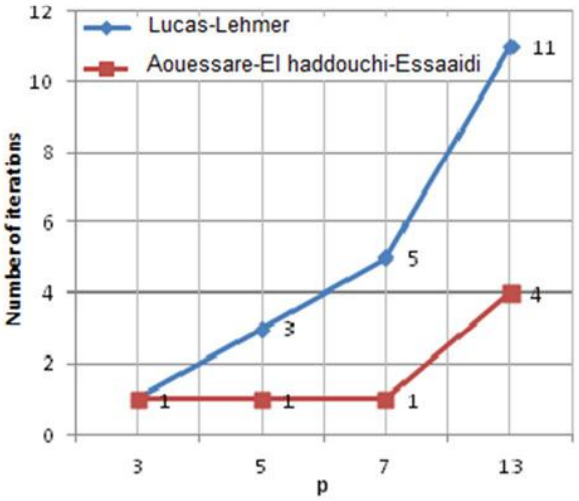

Fig 2: Number of iterations in the primality test versus Mersenne prime number parameter p

The following section will discuss the performance of the proposed primality test in Theorem 1 above, for Mresenne prime numbers. A simple inspection of the expression of the

composition number Kn, defined in this theorem, indicates a complexity order O(n) which is much lower compared to that of Lucas-Lehmer [3,4], namely, O (n)=n² log n log log n.

This result is confirmed through Mersenne numbers tested using both algorithms as shown in Figure 2. It can be easily seen that Aouessare-El Haddouchi-Essaaidi Test is much faster than that of Lucas-Lehmer since the number of iterations required for this test is much lower than that of Lucas-Lehmer's as predicted by the complexity order of this test.

Table 2. Lucas-Lehmer series Sn vs number of digits.

n	S_n	Number of digits
0	4	1
1	14	2
2	194	3
3	37634	5
4	1416317954	10
5	2005956546822746114	19
6	4023861667741036022825635656102100994	37
7	16191462721115671781777559070120513664958590125499158514329308740975788034	74

The other important parameter or indicator related with our primality test algorithm performance is related with the computer memory requirements. Lucas-Lehmer algorithm is very greedy in terms of computer memory since it involves very much large integer numbers for Sn parameter as shown in Table 2 and in Figure 3, even for relatively very small Mersenne prime numbers (e.g. for p = 13 there are 292 digits involved!), compared to the numbers involved in the proposed algorithm, Kn does not exceed 4 digits including the minus sign as shown in Table 1.

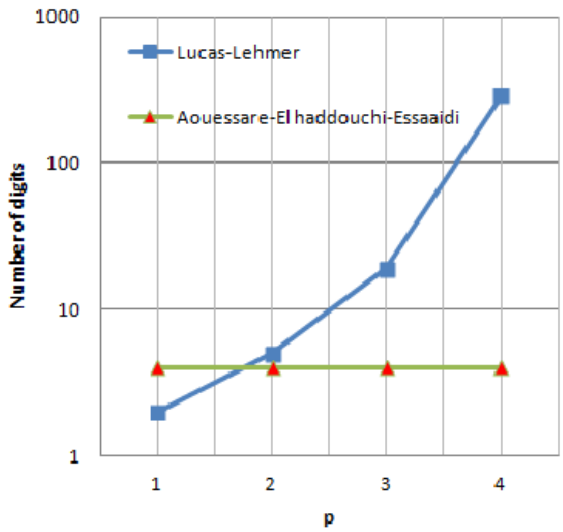

Fig 3: Number of digits of the primality test parameter versus Mersenne prime number parameter p

3. CONCLUSIONS

Aouessare-El Haddouchi-Essaaidi primality Test proposed in this paper provides several very important and key advantages compared to the conventional Lucas-Lehmer test for Mersenne prime numbers in terms of reduced number of computations and number of digits which translates into very fast computations and very low computer memory requirements. These features represent a real breakthrough in primality test for large prime numbers. Thus, it is anticipated that a very important progress in the exploration of very large prime numbers will be achieved with the outstanding implication it involves for information encryption and security and for cybersecurity.

4. REFERENCES

[1]. Grant, G. L. 1997. Understanding digital signatures: establishing trust over the internet and other networks. New York: Computing McGraw-Hill.

[2]. Ferguson, N., Schneier, B., & Kohno, T. 2010. Cryptography Engineering: Design Principles and Practical Applications. New York: John Wiley & Sons.

[3] Dickson, L. E. 1971. History of the theory of numbers, Carnegie Institute of Washington. Reprinted by Chelsea Publishing, New York.

[4]. Williams, H. C.1998. Édouard Lucas and primality testing, Canadian Mathematical Society Series of Monographs and Advanced Texts, 22, Wiley-Interscience, New York.

[5] Bruce, J. W. 1993. A really trivial proof of the Lucas–Lehmer test. The American Mathematical Monthly, 100, 370–371.

[6]. Caldwell, K. 2014. Mersenne primes: History, theorems and lists, http://primes.utm.edu/mersenne.

[7] Aron, J. 2013. New 17-million-digit monster is largest known prime". New Scientist.

[8] Caldwell, K. The largest known prime by year: A brief history, http://primes.utm.edu/notes/by_year.html. (April 2014).

[9] Great Internet Mersenne prime search (GIMPS), http://www.mersenne.org/ (April 2014).