{tag} {/tag}
International Journal of Computer Applications

Volume 100 - Number 3

Year of Publication: 2014

Authors:
Abdelilah Aouessare

Abdeslam El Haddouchi

Mohamed Essaaidi

10.5120/17505-8053
{bibtex}pxc3898053.bib{/bibtex}

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.

References

- Grant, G. L. 1997. Understanding digital signatures: establishing trust over the internet and other networks. New York: Computing McGraw-Hill.
- Ferguson, N. , Schneier, B. , & Kohno, T. 2010. Cryptography Engineering: Design Principles and Practical Applications. New York: John Wiley & Sons.
- Dickson, L. E. 1971. History of the theory of numbers, Carnegie Institute of Washington. Reprinted by Chelsea Publishing, New York.
- Williams, H. C. 1998. Édouard Lucas and primality testing, Canadian Mathematical Society Series of Monographs and Advanced Texts, 22, Wiley-Interscience, New York.
- Bruce, J. W. 1993. A really trivial proof of the Lucas–Lehmer test. The American Mathematical Monthly, 100, 370–371.
- Caldwell, K. 2014. Mersenne primes: History, theorems and lists, http://primes. utm. edu/mersenne.
- Aron, J. 2013. New 17-million-digit monster is largest known prime". New Scientist.
- Caldwell, K. The largest known prime by year: A brief history, http://primes. utm. edu/notes/by_year. html. (April 2014).
- Great Internet Mersenne prime search (GIMPS), http://www. mersenne. org/ (April 2014).

Index Terms

Computer Science Algorithms

Keywords

Prime numbers Mersennes prmes primality test cryptography security and privacy.