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


Index Terms

Computer Science
Algorithms

Keywords
Prime numbers  Mersenne primes  primality test  cryptography  security and privacy.