

1145-11-1467

Gulhan Ayar (gulhanayar@kmu.edu.tr), Karamanoglu Mehmetbey University, Karaman, Turkey, **Kubra Nari*** (nari15@itu.edu.tr), Istanbul Technical University, Istanbul, Turkey, and **Enver Ozdemir** (ozdemiren@itu.edu.tr), Istanbul Technical University, Istanbul, Turkey.
Primality Test with Singular Curves. Preliminary report.

In this work, we develop a method to determine a given odd integer $n = 3 \pmod{4}$ is prime or not. The method will be based on already presented an algorithm for he integers $n = 1 \pmod{4}$. Prime integers are main ingredient of the most popular public key cryptosystems like RSA and Elliptic Curve Cryptosystem. For example, a secure design of an RSA cryptosystem requires prime integers with at least 300 digits. After being employed in cryptography, the prime integers and primality test has been rigorously studied by many researchers. Even though, there are 3 main algorithms being used in practice, finding a practical and deterministic primality test is still considered to be an important problem. In this work, we extend the primality test algorithm for $n = 1 \pmod{4}$ to cover all integers i.e. for $n = 3 \pmod{4}$. (Received September 22, 2018)