

Lect. Dr. Sorin Iftene
Department of Computer Science
"Al.I.Cuza" University
E-mail: siftene@info.uaic.ro

Computational Number Theory, Spring 2017

Homework 3 (10 points)
March 31, 2017

1. Implement the Solovay-Strassen primality test. For computing the Jacobi symbol, use the algorithm discussed in class; (5p)
2. Implement the Lucas-Lehmer primality test for Mersenne numbers. For performing the modular reduction modulo a Mersenne number, use the algorithm discussed in class. (5p)

Due: April 25, 28