University of Limerick
Dr. Bernd Kreussler

22 October 2015
Exercise Sheet 7

MA 6011 (Cryptographic Mathematics)

Solve Problems 1–4 ***before*** *the tutorial on Tuesday, 3 November.*

Problem 1: Evaluate the following Legendre symbols: $\left(\frac{55}{101}\right), \left(\frac{346}{557}\right), \left(\frac{222}{337}\right)$.

Problem 2: Evaluate the following Jacobi symbols: $\left(\frac{17}{2015}\right), \left(\frac{345}{1247}\right), \left(\frac{7811}{35953}\right)$.

Problem 3: Here is a list of all 25 prime numbers less than 100:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Find all primes among them for which both, -1 and 2, are quadratic residues.

Problem 4: Does 33 pass the Solovay-Strassen test to base 5?

Use sage to solve the following ***before*** *we meet for the lab on Tuesday, 27 October.*

Problem 5: Let $p = 97$. For each quadratic residue a between 1 and $p - 1$ print the two solutions to the congruence $x^2 \equiv a \mod p$. In preparation for this, you may calculate all the squares modulo p of the numbers from 1 to $(p - 1)/2$.

Problem 6: For each integer a in the range $1, 2, \ldots, 76$ calculate the Jacobi symbol $\left(\frac{a}{77}\right)$ and determine if the congruence $x^2 \equiv a \mod 77$ has a solution.

Problem 7: Does $n = 409537$ pass the Solovay-Strassen test to base $a = 345678$? Is $a = 1234567345679$ an Euler witness for $n = 10714934881993$?