CRYPTOGRAPHY MISSION 06 SOLUTIONS

Deadline: Thursday, 20 October 2016 at 3:05pm
This mission covers Sections 3.9, 3.10, and 4.2.

1. Graded Problems

1. Given an integer a and an odd prime p. Determine if $x^2 \equiv a \mod p$ has a solution or not. Justify.
   a. $a = 4, p = 11$

   $4^{\frac{11-1}{2}} = 4^5 \equiv 1 \mod 11$, so yes.

   b. $a = 2, p = 19$

   $2^{\frac{19-1}{2}} = 2^9 \equiv 18 \mod 19$, so no.

   c. $a = 3, p = 29$

   $3^{\frac{29-1}{2}} = 3^{14} \equiv 28 \mod 29$, so no.

2. Given an integer a (not congruent to $0 \mod p$) and an odd prime p, recall that the Legendre symbol is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue } \mod p \\ -1 & a \text{ is a quadratic non-residue } \mod p \end{cases}$$

   Evaluate the following:
   a. $\left(\frac{7}{13}\right)$

   We can compute this by hand or use SageMath. The `kronecker` command is the same as the Legendre symbol.
   `kronecker(7,13)` = -1

   b. $\left(\frac{7}{19}\right)$

   `kronecker(7,19)` = 1

   c. $\left(\frac{2}{13}\right)$

   `kronecker(2,13)` = -1

   d. $\left(\frac{14}{13}\right)$

We can use the property that the Legendre symbol is multiplicative to show that $\left(\frac{14}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{7}{13}\right) = (-1)(-1) = 1$

3. Recall that the Law of Quadratic Reciprocity says: Let p and q be odd primes. Then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ \left(-\frac{q}{p}\right) & p \equiv q \equiv 3 \bmod 4 \end{cases}$$

Compute the following. Be sure to show all work.

a. $\left(\frac{97}{101}\right)$

`kronecker(97,101)` $= 1$

b. $\left(\frac{101}{97}\right)$

Since $97 \equiv 1 \bmod 4$, then the answer is still 1.

c. $\left(\frac{5}{103}\right)$

`kronecker(5,103)` $=$ -1.

d. $\left(\frac{103}{5}\right)$

Since $5 \equiv 1 \bmod 4$, then the answer is still -1.

e. $\left(\frac{69}{389}\right)$

$$\left(\frac{69}{389}\right) = \left(\frac{3 \cdot 23}{389}\right) = \left(\frac{3}{389}\right)\left(\frac{23}{389}\right)$$

Note that $3, 23$, and 389 are all odd primes. 3 and 23 are $\equiv 3 \mod 4$, but $389 \equiv 1 \mod 4$, so we have:

$$\left(\frac{3}{389}\right)\left(\frac{23}{389}\right) = (-1)(-1) = 1$$