CRYPTOGRAPHY MISSION 06 DOSSIER

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

Check one:

☐ I received help from the following classmate(s) on this assignment:

_____.

☐ I did not receive any help on this assignment.

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. $a = 4, p = 11$

b. $a = 2, p = 19$

c. $a = 3, p = 29$

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. $\left(\frac{7}{13}\right)$

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

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

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

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

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

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

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

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

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 3.13: # 29, 30, 31, 32
- Section 3.14: # 11, 12, 13