Homework 3

Math 124, Fall 2004

Due Wednesday, October 12

No late assignments will be accepted as solutions will be posted on Thursday morning. Good luck!

1. Consider the prime 73.
   (a) Show that 10 and 2 are solutions of $x^8 \equiv 1$ and $x^9 \equiv 1 \pmod{73}$ respectively.
   (b) Find the index of 10. Show that 8 divides the index of 2.
   (c) Show that 20 is a primitive root modulo 73.
   (d) Which of the following equations have a solution?

$$\begin{aligned} x^{104} &\equiv 2 \mod 73 \\ x^{207} &\equiv 10 \mod 73 \\ x^{205} &\equiv 47 \mod 73 \\ x^{104} &\equiv 57 \mod 73 \end{aligned}$$

2. Consider the equation

$$x^k \equiv a \mod p. \tag{1}$$

   (a) Prove that there are solutions to (1) if and only if

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \mod p$$

   (b) Prove that there are either zero or $(k, p-1)$ solutions to the equation (1). Write down all possible the solutions in terms of g a primitive root of p.
   (c) How many solutions do the equations

$$\begin{aligned} x^{20} &\equiv 6 \mod 101 \\ x^{20} &\equiv -6 \mod 101 \\ x^8 &\equiv -1 \mod p \end{aligned}$$

   have?

3. (a) Calculate the following Legendre symbols.

$$\left(\frac{-26}{73}\right) \quad \left(\frac{19}{73}\right) \quad \left(\frac{33}{73}\right).$$

(b) Which of the following equations are solvable?

i. $x^2 \equiv -7 \mod 1009$

ii. $x^2 \equiv 5 \mod 229$

iii. $x^2 \equiv 125 \mod 227$

[Hint : 1009, 229 and 227 are not prime.]

(c) Find all primes p such that

$$\left(\frac{10}{p}\right) = 1$$

4. (a) Prove that they are infinitely many primes of the form $3n - 1$.

(b) Prove that they are infinitely many primes of the form $3n + 1$.

i. Find an integer a that is a quadratic residue modulo p if and only if $p = 3n + 1$.

ii. Assume there are only finitely many primes $\{p_1, \ldots, p_k\}$ of the form $3n + 1$ and construct an integer n such that

A. None of the p_i's divide n.

B. Any p dividing n has a as a quadratic residue and hence is of the form $3n + 1$.