CS 235
Spring 2010

Assignment 3

Date Due: Thursday, February 18

Reading: Read Chapter called Rings and Fields (Chapter 7 or Chapter 8 depending on which edition of the text you have)

Problems:

1. Solve for x in 81x = 1 (mod 43)

2. Find inverses of 2, 4, 5, and 7 in Z_{11}.

3. Which elements in Z_{14} have inverses ? Find the inverses in each case.

4. Let a, b, n, k∈ Z with n, k> 0 and gcd(n, k) = 1. Show that a ≡ b (mod n) and a ≡ b (mod k) implies a ≡b (mod nk)

5. Prove that for any prime p and integer x, if x^2 ≡ 1 (mod p) then x ≡ 1 (mod p) or x ≡ -1 (mod p).

   Hint: For any x, (x^2 -1) = (x+1)(x-1).

6. Show that if gcd(a,m) > 1 then the equation $a^x \equiv 1$ (mod m) is not solvable for any integer x>0.

7. Show that the equation $x^2 = y^2 = 4z - 1$ has no solutions where x,y and z are integers.

   Hint: Use mod 4 arithmetic and consider the values of $(2w)^2$ mod 4 and of $(2w+1)^2$ mod 4 for any integer w.

8. A restaurant sells chicken wings in order of size 9 and 20.

   What is the largest number of chicken wings that you cannot order exactly ?

9. Note: A number b is called a primitive element of Z_m if the set $\{0, b, b^2, ..., b^{m-1}\}$ is a complete set of representatives of Z_m.

   i. Find a primitive element of Z_{11}, and verify your answer.

   ii. Find all the primitive roots (mod 7) which are between 0 and 7, verify your answers.

10. Assume S is a complete set of representatives for Z_m and that a is such that (a,m) = 1, then prove that aS = { as | s ∈ S} is also a complete set of representatives for Z_m.