Homework Number: 3  
Name: Jose Luis Tejada  
ECN Login: tejada  
Due Date: Thursday 02/06/2020 at 4:29PM

*Questions:*

1. Show whether or not the set of remainders Z\_12 forms a group with either one of the modulo addition or modulo multiplication operations.

Z\_12 = {0,1,2,3,4,5,6,7,8,9,10,11}, Forms a group using addition only since for the multiplication operator, the multiplicative inverse of 4,6,8 does not exist, thus not forming a group.

1. Compute gcd(29495, 16983) using Euclid’s algorithm. Show all the steps.

gcd(29495, 16983) = gcd(16983, 29495%16983) = gcd(16983, 12512)

= gcd(12512, 16983 % 12512) = gcd(12512, 4471)

= gcd(4471, 12512% 4471) = gcd(4471, 3570)

= gcd(3570,4471 % 3570) = gcd(3570,901)

= gcd(901, 3570 % 901) = gcd(901,867)

= gcd(867, 901 % 867) = gcd(867, 34)

= gcd(34, 867%34) = gcd(30,17)

= gcd(17, 34%17) = gcd(17,0)

= 17

1. With the help of Bezout’s identity, show that if c is a common divisor of two integers a, b > 0, then c | gcd(a,b)  (i.e. c is a divisor of gcd(a,b)).

Let d = gcd(a,b)

Therefore d|a, d|b.

Based on bezouts identity:

Common divisor divides the integer combination: c|a and c|b therefore c |

Therefore: c|d

1. Use the Extended Euclid’s Algorithm to compute by hand the multiplicative inverse of 25 in Z\_28 . List all of the steps.

Multiplicative Inverse of 25 in Z\_28:

gcd(25, 28) = gcd(28, 25), Residue: 25 = (1)\*25 + (0)\*28

= gcd(25,3), Residue: 3 = (1)\*28 + (-1)\*25

= (1)\*28 + (-1)\* ((1)\*25 + (0)\*28)

= (1)\*28 + (-1)\*25

= gcd(3, 1), Residue: 1 = (1)\*25 + (-8)\*3

= (1)\*25 + (-8)\* ((1)\*28 + (-1)\*25)

= (9)\*25 + (-8)\*28

The multiplicative inverse of 25 in Z\_28 is 9.

1. In the following, find the smallest possible integer x. Briefly explain (i.e. you don’t need to list out all of the steps) how you found the answer to each. You should solve them without using brute-force methods:
   1. 8x ≡ 11 (mod 13)
   2. 5x ≡ 3 (mod 21)
   3. 8x≡9(mod7)

*Programming Printout:*

*#!/usr/bin/env python3***def** determine\_field(n):  
 *#For each element, determine if all elements of Zn -excluding 0- have a multiplicative inverse  
 #We can do this by determining whether an element is relatively prime to n.* z\_index = 1  
 **while**(z\_index < n):  
 *#Perform gcd(z,k=n) and determine if == 1, if so there is a multiplicative inverse,  
 #Otherwise there is not, which means it is a Comunitative ring.* k = n  
 z = z\_index  
 **while**(k):  
 z,k = k, z % k  
 **if**(z != 1):  
 print(**"ring"**)  
 **return** z\_index += 1  
 print(**"field"**)  
 **return  
  
if** \_\_name\_\_ == **"\_\_main\_\_"**:  
 num = input(**"Enter a number n:"**)  
 **if** num.isdigit():  
 determine\_field(int(num))  
 **else**:  
 print(**"Input must be a positive integer"**)  
 exit(1)