Homework Number: 03

Name: Tycho Halpern

ECN Login: thalper

Due Date: February 3, 2022

1.) Show whether or not the set of remainders Z21 forms a group with the modulo addition operator. Then show whether or not Z21 forms a group with the modulo multiplication operator.

Z21 does form a group with the binary operator of addition. It is associative, has an identity element of 0, and each element has an additive inverse. The inverse of an element i is (21 – i). For example the inverse of 12 is (21-12) = 9. 12+9 = 0 in Z21

Z21 also forms a group with the binary operator of multiplication. It is associative, has an identity element of 1, and each element other than 0 has a multiplicative inverse. The MI of an element i can be found using the extended Euclidean algorithm.

2.) The identity element for unsigned integers under the gcd operator is 1, and the inverse for any i in W is 1 because gcd(i,1) = 1 which is the identity element so W is a group under the gcd operator.

3.) Gcd(21609,18432) = gcd(18432, 21609%18432) = gcd(18432, 3177)
gcd(18432, 3177) = gcd(3177,18432%3177) = gcd(3177,2547)
gcd(3177,2547) = gcd(2547,3177%2547) = gcd(2547, 630)
gcd(2547, 630) = gcd(630, 2547%630) = gcd(630, 27)
gcd(630, 27) = gcd(27, 630%27) = gcd(27, 9)
gcd(27, 9) = gcd(9,27%9) = gcd(9,0) = 9

gcd(21609,18432) = 9

4.) Gcd(35,24)

Gcd(35,24)	24 = 1x24 + 0x35
Gcd(24,11)	11 = -1x24 + 1x35
Gcd(11,2)	2 = 1x24 –2(-1x24 + 1x35)
	2 = 1x24 +2x24 – 2x35
	2 = 3x24 – 2x35
Gcd(2,1)	1 = 11 - 5x2
	1 = -1x24 + 1x35 – 5(3x24 – 2x35)
	1 = -16x24 + 11x35

Multiplicative inverse is -16
-16 % 35 = 19
Multiplicative inverse is 19

5.)

a. 6x = 3 in mod 23
   3 is not a multiple of 6, so add 23 to 3 until it is a multiple of 6
   26 no
   49 no
   72 yes, 6*12 = 72
   X = 12
b. 7x = 11 in mod 13
   11 is not a multiple of 7, so add 13 to 11 until it is a multiple of 7
   24 no
   37 no
   50 no
   63 yes, 7*9 = 63
   X = 9
c. 5x = 7 in mod 11
   7 is not a multiple of 5, so add 11 to 7 until it is a multiple of 5
   18 no
   29 no
   40 yes, 5*8 = 40
   X = 8