ECE 404 Homework

Homework Number: 3
Name: Dylan Huynh
ECN Login: huynh38
Due Date: 2/2/2023

1. A group must have a binary operator that has closure, associativity, an identity element and an inverse element for each element in the set. The set of remainders Z_{18} with the modulo addition operator forms a group. It has closure, because the modulo operator guarantees the remainder to be in the set, by definition. It has associativity because the addition operation has no difference in order between itself, in other worse one addition can happen before the other and vise versa, and the sum will have no difference. An identity element exists because 0 added to any number will result in the same number, which is the definition of an identity element. Each element has an inverse because each number from [0 - 17], which we can denote as w, has an inverse element which is equal to 18 - w. For example, the inverse element of 3 is 18 - 3 = 15, which is obvious. These 4 properties show that the set of remainders Z_{18} with the modulo addition operator forms a group.
The set of remainders Z_{18} with the modulo multiplication operator does not form a group. We know that a operator only has to violate one rule to make the set not form a group, which in this case is the inverse element for each element in the set. This is because the identity element is 1, because any number multiplied by 1 is itself. Take for example 9, which is in the set of remainder Z_{18}, only has 2 unique products when modularized, 0 and 9. We can see here that there is no number that will create the identity element with 9 in the set, thus showing that the set of remainders Z_{18} with the modulo multiplication is not a group.

2. A group must have a binary operator that has closure, associativity, an identity element and an inverse element for each element in the set. There has to be a common divisor, which requires an integer less than the smallest number to be compared to in the GCD so it has closure, and since there has to be a common divisor between 3 numbers, it is associative. The identity element is 0 because an element *a* can always be divided by *a*, as can 0. This means however, that there can be no inverse elements for this set, because 0 cannot be a output of a gcd because dividing by 0 cannot return an integer. **So W is not a set**.

3. gcd(10946, 19838)| (19838)mod 10946 = 8892
gcd(8892, 10946)| (10946)mod 8892= 2054
gcd(2054, 8892)| (8892)mod 2054= 676
gcd(676, 2054)| (2054)mod 676 = 26
gcd(26, 676)| (676)mod 26 = 0
gcd(10946, 19838) = 26

4. First, we know that 19 is relatively prime to 35, so a multiplicative inverse must exist
gcd(19, 35)
gcd(16, 19) | residue 16 = 1*35 - 1*19
gcd(3, 16) | residue 3 = 1*19 - 1 * 16
| = 1*19 - (1*35 - 1*19)

	= (-1)*35 + 2*19
gcd(1, 3)	residue 1 = 1*16 - 5*3
	= 1*35 - 1*19
	-5*((-1)*35 + 2*19)
	= (-11)*19 + 6*35
	= 24*19 + 6*35

The multiplicative inverse of 19 modulo 35 is 24

5. (a) 6 and 23 are co prime, which means that x must be in the range of [0,22], because anything past that will repeat, and every remainder within this range is unique.
We want the equation 3 = x * 6 + y * 23 so we can find x. However, the GCD of these two number makes 1, so we multiply 3 to both sides to get the x. The Bezout identity is 1 = 6*4 - 23*1 which makes **x =12**. We can check by seeing that 12 * 6 = 72 mod 23 = 3
(b) For this equation we want to find 11 = x*7 + y*13. The Bezout identity yields, 1 = 2*7 - 1*13. We multiply 2 by 11 to get 22, and then modularize 22 to get 9. 9 * 7 = 63, and 63 mod 13 = 11.
x = 9
(c) For this we need 7 = x*5 + 11*y, the Bezout identity is 1 = 5 * 9 + 11*4. We multiply 9 * 7 mod 11 to get 8, and **x = 8**. We can check by 5*8 = 40 mod 11 = 7.