ECE 404 HW3

Nimal Padmanabhan

February 02, 2023

1 Theory Problems

1.1 Modulo Addition

1. Show whether or not the set of remainders Z_{18} forms a group with the modulo addition operator. Then show whether or not Z_{18} forms a group with the modulo multiplication operator.
   Closure
   It meets closure under the modulo addition operator because if you take two elements a and b in the set and apply the modulo addition operator, the result of that operation is also in the set, which in this case repeats after 18 elements as shown in the table below.

Z_{18}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Additive Inverse	0	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

   Associativity
   For any three elements in this set (a, b, c), (a + b) + c = a + (b + c).
   Existence of Identity Element
   In this set, the identity element is 0, so any element in Z_{18} that has the modulo addition operator on 0 will the element itself. (a + 0 (mod 18) = a (mod 18)).
   Existence of Inverse Element For any element in this set, there exists corresponding element b that forms $a + b \equiv 0$ (mod 18)

1.2 Modulo Multiplication

The set that forms under modulo multiplication fails to form a group because not every element in the set has a multiplicative inverse, which violates the existence of inverse element rule.

Z_{18}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Multiplicative Inverse	-	1	-	-	-	11	-	13	-	-	-	5	-	7	-	-	-	17

2. Is the set of all unsigned integers W a group under the $gcd(\cdot)$ operation? Why or why not? **Hint:** Find the identity element for $\{W, gcd(\cdot)\}$
   The identity element for $\{W, gcd(\cdot)\}$ is 1; however, it is not the GCD of any two elements in this set, which violates the existence of the inverse element because not every element in this set has an inverse.

3. Compute $gcd(10946, 19838)$ using Euclid's algorithm. Show all of the steps.

```
gcd(10946, 19838) = gcd(19838, 10946)
gcd(10946, 8892) = gcd(8892, 2054)
gcd(2054, 676) = gcd(676, 26)
gcd(26, 0) = 26
```

4. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 19 in Z_{35}. List all of the steps.

```
gcd(19, 35) = gcd(35, 19)
gcd(35, 19) | residue 19 = 1×19 + 0x35
gcd(19, 16) | residue 16 = −1×19 + 1×35
gcd(16, 3)  | residue 3 = 1×19 − 1×16
            |              = 1×19 − 1×(1×35 − 1×19)
            |              = 2×19 − 1×35
gcd(3, 1)   | residue 1 = 16 − 5×3
            |              = (1×35 − 1×19) − 5×(2×19 − 1×35)
            |              = −11×19 + 6×35
            |              = 24×19 + 6×35
```

The additive inverse of -11 is 24 (-11 + 35 = 24).

The multiplicative inverse of 19 in Z_{35} is 24.

5. 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 simply plugging in arbitrary values for x until you get the correct value:

   (a) $6x \equiv 3 \pmod{23}$
   $x = 12$
   You first rewrite $6x \equiv 3 \pmod{23}$ into $6x \pmod{23} = 1$
   The value of x that satisfies this is 4. Then, you multiply 4 with 3, which results in $x = 12$ and is in the Z_{23} set.

   (b) $7x \equiv 11 \pmod{13}$
   $x = 9$
   Same approach as the first problem, but when you multiply 2 with 11, it is outside the Z_{13} set, so you do 22 mod 13, which results in $x = 9$.

   (c) $5x \equiv 7 \pmod{11}$
   $x = 8$
   Similar scenario as the previous problem, multiplying 9 with 7 results in 63, which is outside the Z_{11} set, so 63 mod 11 results in $x = 8$.

2 Programming Problem

Explanation of Code:
For the programming portion, we had to rewrite the multiplicative inverse function and division and multiplication functions using bit wise operations. Descriptions for the multiplication and division functions are available in the multinv.py file.