Theory:

PREKSHAA
VEERARAGAVAN

HW - 3

I. Theory Problems

1) Z_{18} forms a group with modulo addition operator? Yes
Z_{18} forms a group with modulo multiplication operator? No

Group: To form a group, should satisfy 4 properties — closure, associativity, guaranteed existence of unique identity element, inverse element.

$Z_{18} = \{0, 1, 2, \dots, 17\}$

It is closed for modulo addition, since for any $a, b \in Z_{18}$, ~~(a+b) mod n~~
$(a+b) \bmod n = c \bmod n \in Z_{18}$ eg) $(1+2) \bmod 18 = 3 \bmod 18 \in Z_{18}$

It is associative for modulo addition, for any $a, b, c \in Z_{18}$,

$[[(a+b) \bmod n] + c \bmod n]_{\bmod n} = [a \bmod n + (b+c) \bmod n] \bmod n.$

eg) $[((0+8) \bmod 18) + 5 \bmod 18]_{\bmod 18}$ $[0 \bmod 18 + (8+5) \bmod 18] \bmod 18$

The unique identity element is 0, and there exists an inverse element for each element, with regard to modulo addition.

$\therefore$ Z_{18} forms a group with modulo addition operator.

But, Z_{18} does not form a group with modulo multiplication operator, since the inverse of ~~the~~ some elements does not exist in the set,
eg) 0, doesnot have an inverse element for modulo multiplication.

2. $\gcd(36{,}459, 27{,}828) = \gcd(27{,}828, 36{,}459 \bmod 27{,}828)$.
$= \gcd(27{,}828, 8631) = \gcd(8631, 27828 \bmod 8631)$
$= \gcd(8631, 1935) = \gcd(1935, 8631 \bmod 1935)$
$= \gcd(1935, 891) = \gcd(891, 1935 \bmod 891)$
$= \gcd(891, 153) = \gcd(153, 891 \bmod 153)$
$= \gcd(153, 126) = \gcd(126, 153 \bmod 126) = \gcd(126, 27)$
$= \gcd(27, 126 \bmod 27) = \gcd(27, 18) = \gcd(18, 27 \bmod 18) = \gcd(18, 9)$
$= \gcd(9, 18 \bmod 9) = \gcd(9, 0) = 9.$

4. Extended Euclid's Algorithm to compute multiplicative inverse of 27 modulo 32

gcd (27, 32)

= gcd (32, 27)

= gcd (27, 5)

= gcd (5, 2)

= gcd (2, 1)

residue 27 = $1 \times 27 + 0 \times 32$

residue 5 = $-1 \times 27 + 1 \times 32$

residue 2 = $1 \times 27 + (-5) \times 5$

$= 1 \times 27 + (-5) \times (-1 \times 27 + 1 \times 32)$

$= 1 \times 27 + 5 \times 27 - 5 \times 32$

$= 6 \times 27 - 5 \times 32$

residue = 1 = $1 \times 2 - 1 \times 1$

$= 1 \times (6 \times 27 - 5 \times 32) - 1 \times (1 \times 5 - 2 \times 2)$

$= 6 \times 27 - 5 \times 32 - 1 \times 5 + 2 \times (6 \times 27 - 5 \times 32)$

$= 6 \times 27 - 5 \times 32 - (-1 \times 27 + 1 \times 32) + 2(6 \times 27 - 5 \times 3$

$= 6 \times 27 - 5 \times 32 + 1 \times 27 - 1 \times 32 + 12 \times 27 - 10 \times 32$

$= 19 \times 27 - 16 \times 32$

$\therefore$ Multiplicative inverse = 19.

5. a. $9x \equiv 11 \bmod 13$

$\gcd(9, 13) = \gcd(13, 9)$

$= \gcd(9, 4)$

residue $9 = 1\times9 + 0\times13$

r $4 = -1\times9 + 1\times13$

$= \gcd(4, 5) = \gcd(5, 4)$

r $5 = 1\times9 - (-1\times9 + 1\times13)$

$= 2\times9 - 1\times13$

$= \gcd(4, 1)$

r $1 = 2\times9 - 1\times13 - (-1\times9 + 1\times13)$

$= 3\times9 - 2\times13$

$\therefore$ Multiplicative inverse of $9 = 3$.

$\therefore \quad 9(3)x \equiv 11(3) \bmod 13$

$(1)x = 33 \bmod 13$

$\therefore \quad \underline{x = 7}$

b. $6x \equiv 3 \bmod 23$

$\gcd(6, 23) = \gcd(23, 6)$

$= \gcd(6, 17) = \gcd(17, 6)$

$= \gcd(6, 11) = \gcd(11, 6)$

$= \gcd(6, 5)$

$= \gcd(5, 1)$

residue $6 = 1\times6 + 0\times23$

r $17 = -1\times6 + 1\times23$

r $11 = (-1\times6 + 1\times23) - 1\times6$

$= -2\times6 + 1\times23$

r $5 = (-2\times6 + 1\times23) - 1\times6$

$= -3\times6 + 1\times23$

r $1 = 1\times6 - (-3\times6 + 1\times23)$

$= 4\times6 - 1\times23$

$\therefore$ MI of $6 = 4$.

$\therefore \quad 6(4)x \equiv 3(4) \bmod 23$

$\therefore \quad x = 12 \bmod 23$

$\therefore \quad \underline{x = 12}$

c. $5x \equiv 9 \bmod 11$

$\gcd(5, 11) = \gcd(11, 5)$

$= \gcd(5, 6) = \gcd(6, 5)$

$= \gcd(5, 1)$

residue $5 = 1\times5 + 0\times11$

residue $6 = -1\times5 + 1\times11$

residue $1 = -1\times5 + 1\times11 - 1\times5$

$= -2\times5 + 1\times11$

$\therefore$ MI of $5 = -2$

$\therefore \quad 5(-2)x = 9(-2) \bmod 11$

$\therefore \quad x = -18 \bmod 11$

$\therefore \quad \underline{x = 4}$

Programming:
Code:

```
#####
#Homework Number: 3
#Name: Prekshaa Veeraragavan
#ECN login: pveerar
#Due Date: February 11, 2021
#####
#!/usr/bin/env python 3.7



## FindMI.py
#reference for mult: https://stackoverflow.com/questions/3722004/how-to-perform-multiplication-using-bitwise-
operators

import sys
```

```
if len(sys.argv) != 3:
    sys.stderr.write("Usage: %s   <integer>   <modulus>\n" % sys.argv[0])
    sys.exit(1)

NUM, MOD = int(sys.argv[1]), int(sys.argv[2])

def mult(x, y):
    r = 0   ##var to return
    while (y > 0):      ##for positive ints
        if (y & 1):     ##check if odd
            r = r + x   ##add 1x to itself

        x = x << 1      ##multiply by 2
        y = y >> 1      ##divide by 2, because multiplicatio(by 2) taken care of

    return r

def div(x, y):

    quo = 0 ##quotient

    if (x < y):
        quo = 0
    elif (x == y):
        quo = 1
    else:

        while (x > y):


            x = x - y      ##remove 1y from x
            quo = quo + 1   ##update quotient odd



    return quo
```

```python
def MI(num, mod):
    '''
    This function uses ordinary integer arithmetic implementation of the
    Extended Euclid's Algorithm to find the MI of the first-arg integer
    vis-a-vis the second-arg integer.
    '''
    NUM = num; MOD = mod
    x, x_old = 0, 1
    y, y_old = 1, 0
    while mod:
        q = div(num, mod)
        num, mod = mod, num % mod
        x, x_old = x_old - mult(x, q), x
        y, y_old = y_old - mult(y, q), y
    if num != 1:
        print("\nNO MI. However, the GCD of %d and %d is %u\n" % (NUM, MOD, num))
    else:
        MI = (x_old + MOD) % MOD
        print("\nMI of %d modulo %d is: %d\n" % (NUM, MOD, MI))

MI(NUM, MOD)
```