Homework Number: hw03

Name: Shu Hwai Teoh

ECN Login: teoh0

Due Date: Thursday 02/06/2020 at 4:29PM

1. Theory Problems

   I. Show whether or not the set of remainders Z_{12} forms a group with either one of the modulo addition or modulo multiplication operations.

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$$

i. Z_{12} forms a group with modulo addition

1. Closure: a = x mod 12, b = y mod 12, a+b = (x mod 12) + (y mod 12) = (x+y) mod 12. x+y is an integer and any integer divided by 12 must has a remainder $\in Z_{12}$. $\therefore$ Z_{12} is closed.
2. Associativity:
   w = 12a + r_a, x = 12b + r_b, y = 12c + r_c
   w+x = 12a + r_a + 12b + r_b
   (w+x)+y = 12a + r_a + 12b + r_b + 12c + r_c
   x+y = 12b + r_b + 12c + r_c
   w+(x+y) = 12a + r_a + 12b + r_b + 12c + r_c
   (w+x)+y = w+(x+y)
   ∴[(w+x)+y] mod 12 = [w+(x+y)] mod 12
3. existence of a unique identity element:
   For each w$\in Z_{12}$, 0+w = w+0 = w
   (0+w) mod n = (w+0) mod n = w mod n
4. existence of an inverse element for each element:
   For each w$\in Z_{12}$, there exists a z$\in Z_{12}$ such that (w+z)mod12 = 0.
   0+0=0, [1+(12-1)] mod 12 =0, [2+(12-2)] mod 12 =0…
   [5+(12-5)] mod 12 =0, [6+(12-6)] mod 12 = 0

ii. Z_{12} does not form a group with modulo multiplication

Existence of an inverse element is not for each element. Zero doesn’t have multiplicative inverse.

II. 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(34,17)

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

III. 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)).

A>b, a=mb+r, common divisor of a and b is the common divisor of a, b, r

IV. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 25 inZ_{28}. List all of the steps.

gcd(28,25)= gcd(25,3) residue 3=1$\times 28 - 1\times 25$

= gcd(3,1) residue 1=1$\times 25 - 8 \times 3$

=1$\times 25 - 8 \times (1 \times 28 - 1 \times 25)$

=9$\times 25 - 8 \times 28$

So the multiplicative inverse of 25 in Z_{28} is 9.

V. 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:

(a) 8x $\equiv$ 11 (mod 13)

$8^{-1} \times$ 8x $\equiv$ 8^{-1} ×11 (mod 13)

gcd(13,8) = gcd(8,5) residue 5 = 1$\times 13 - 1 \times 8$

= gcd(5,3) residue 3 = 1$\times 8 - 1 \times 5 = 2 \times 8 - 1 \times 13$

= gcd(3,2) residue 2 = 1$\times 5 - 1 \times 3 = 2 \times 13 - 3 \times 8$

= gcd(2,1) residue 1 = 1$\times 3 - 1 \times 2 = 5 \times 8 - 3 \times 13$

X = 8^{-1} ×11 mod 13= $5 \times 11 \bmod 13 = 3$

(b) 5x $\equiv$ 3 (mod 21)

21+1-5=17

X = $5^{-1} \times 3$ mod 21= $17 \times 3 \bmod 21 = 9$

(c) 8x $\equiv$ 9 (mod 7)

Gcd(8,7) = gcd(7,1) residue 1 = 1$\times 8 - 1 \times 7$

X = $8^{-1} \times 9$ mod 7= $1 \times 9 \bmod 7 = 2$

2. Programming Problem

```
#!/usr/bin/env/python3

def prime(number):
    factor = 2
    while factor <= int(number**0.5):
        if number%factor == 0:
            print("ring")
            return
        else:
            factor += 1
    print("field")
    return


if __name__ == "__main__":
    n = input("Enter an integer smaller than 50:")
    prime(int(n))
```