ECE 404 Homework 3

Elias Talcott

February 6, 2020

Contents

1 Theory Problems

1.1 Problem 1

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

Solution

1.2 Problem 2

Compute $gcd(29495, 16983)$ using Euclid's Algorithm. Show all the steps.

Solution

1.3 Problem 3

With the help of Bezout's identity, show that if c is a common divisor of two integers $a, b > 0$, then $c \mid gcd(a, b)$ (i.e. c is a divisor of $gcd(a, b)$)

Solution

1.4 Problem 4

Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 25 in $Z28$. List all of the steps.

Solution

1.5 Problem 5

In the following, find the smallest possible integer x. Briefly explain how you found the answer to each. You should solve them without using brute-force methods.

(a) $8x \equiv 11 \pmod{13}$

(b) $5x \equiv 3 \pmod{21}$

(c) $8x \equiv 9 \pmod{7}$

Solution

(a)

(b)

(c)

2 Programming Problem

Write a program that takes as input a small integer n (say, smaller than 50) and determines if Zn is a field or only a commutative ring. Assume that the operators are modulo n addition and modulo n multiplication. The program should prompt the user to enter the number. Depending upon the input n, it should correctly print out either “field” or “ring”.

2.1 Python Code

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

# Homework Number: 3
# Name: Elias Talcott
# ECN Login: etalcott
# Due Date: February 6, 2020

# Input integer n
n = "-1"
while not n.isdigit() or eval(n) < 1:
    n = input("Enter␣a␣positive␣integer:␣")
    if not n.isdigit() or eval(n) < 1:
        print("{}␣is␣not␣a␣positive␣integer.".format(n))
n = eval(n)

# Check if n is prime
if n < 2:
    prime = False
elif n == 2:
    prime = True
elif n > 2:
    prime = True
    for i in range(2, n // 2):
        if n % i == 0:
            prime = False
            break

# If n is prime, then Zn is a finite field, else it is a ring
if prime:
    print("field")
else:
    print("ring")
```

2.2 Code Explanation

If an integer n is prime, then its set of residues Z_n along with the addition and multiplication operators form a finite field. This is the case because a prime modulus is relatively prime with each member of its set of residues. If a number is relatively prime with the modulus, then it has a multiplicative inverse (a requirement for a ring to become a field).

My solution simply checks whether the modulus is prime or not. If it is prime, the program prints “field”. If it is not prime, the program prints “ring”.