ECE 404 Homework #3

Due: Thursday 02/11/2021 at 5:59PM

This homework covers topics related to finite fields.

Theory Problems

Solve the following problems.

$= \{0, 1, 2, 3, \ldots, 17\}$

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.

2. Compute $gcd(36459, 27828)$ using Euclid's algorithm. Show all of the steps.

3. Is the set of all unsigned integers $\mathbb{W}$ a group under the $gcd(\cdot)$ operation? Why or why not? (**Hint**: Find the identity element for $\{\mathbb{W}, gcd(\cdot)\}$.)

4. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 27 in Z_{32} . List all of the steps.

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) $9x \equiv 11 \pmod{13}$

   (b) $6x \equiv 3 \pmod{23}$

   (c) $5x \equiv 9 \pmod{11}$

Programming Problem

Rewrite and extend the Python (or Perl) implementation of the *binary* GCD algorithm presented in Section 5.4.4 so that it incorporates the Bezout's Identity to yield multiplicative inverses. In other words, create a binary version of the multiplicative-inverse script of Section 5.7 that finds the answers by implementing the multiplications and division as bit shift operations.

Your script should be named `mult_inv.py/pl` and accept two command-arguments:

```
mult_inv.py a b
```

Which should print the multiplicative inverse of `a` mod `b`

1) CLOSURE: $(17+17) \% 18 = 16 \in Z_{18}$
17+17 IS THE BIGGEST SUM POSSIBLE FROM Z_{18}. THEREFORE, SINCE ITS SUM MOD 18 IS IN Z_{18}, ALL OTHER COMBOS WILL HAVE THE SAME OUTCOME AND BE IN Z_{18}

Z_{18} SATISFIES CLOSURE IN MODULO ADDITION

ASSOCIATIVITY:

$$[(15+16)+17] \% 18 = 12$$

$$[15+(16+17)] \% 18 = 12$$

Z_{18} SATISFIES ASSOCIATIVITY IN MODULO ADDITION BECAUSE ADDITION IS ALREADY ASSOCIATIVE SO THE END RESULT IS THE SAME NO MATTER THE GROUPING

IDENTITY ELEMENT:

0 IS THE IDENTITY ELEMENT

AS $(a+0) \% 18 = a$

INVERSE ELEMENT:

ELEMENT	INVERSE
0	0
1	17
2	16
3	15
4	14
5	13
6	12
7	11
8	10
9	9
10	8
11	7
12	6
13	5
14	4
15	3
16	2
17	1

ALL ELEMENTS HAVE AN INVERSE FOR MODULO ADDITION

CLOSURE: $(17 \times 17) \% 18 = 1 \in \mathbb{Z}_{18}$

17×17 IS THE BIGGEST PRODUCT POSSIBLE FROM $\mathbb{Z}_{18}$. THEREFORE, SINCE ITS PRODUCT MOD 18 IS IN $\mathbb{Z}_{18}$, ALL OTHER COMBOS WILL HAVE THE SAME OUTCOME AND BE IN $\mathbb{Z}_{18}$

$\mathbb{Z}_{18}$ SATISFIES CLOSURE IN MODULO MULTIPLICATION

ASSOCIATIVITY:

$$[(15 \times 16) \times 17] \% 18 = 12$$
$$[15 \times (16 \times 17)] \% 18 = 12$$

$\mathbb{Z}_{18}$ SATISFIES ASSOCIATIVITY IN MODULO MULTIPLICATION BECAUSE MULTIPLICATION IS ALREADY ASSOCIATIVE SO THE END RESULT IS THE SAME NO MATTER THE GROUPING

IDENTITY ELEMENT:

1 IS THE IDENTITY ELEMENT

$$(a \times 1) \% 18 = a$$

INVERSE ELEMENT:

NOT ALL ELEMENTS HAVE AN INVERSE

ELEMENT	INVERSE
0	
1	1
2	
3	
4	
5	11
6	
7	13
8	
9	
10	
11	5
12	
13	7
14	
15	
16	
17	17

$\boxed{\text{$\mathbb{Z}_{18}$ FORMS A GROUP WITH MODULO ADDITION OPERATOR BUT $\mathbb{Z}_{18}$ DOES NOT FORM A GROUP WITH MODULO MULTIPLICATION OPERATOR}}$

2) $\gcd(36459, 27828)$

$\gcd(27828, 8631)$

$\gcd(8631, 1935)$

$\gcd(1935, 891)$

$\gcd(891, 153)$

$\gcd(153, 126)$

$\gcd(126, 27)$

$\gcd(27, 18)$

$\gcd(18, 9)$

$\gcd(9, 0)$

$\boxed{\gcd(36459, 27828) = 9}$

3) THE IDENTITY IS 0, SINCE $\gcd(a,0) = a$.
THIS MEANS THE SET W DOES NOT FORM A GROUP UNDER
THE gcd(·) OPERATION. THIS IS BECAUSE THERE IS NO WAY
TO END UP WITH $\gcd(a,b) = 0$ NO MATTER WHAT a AND b ARE.

4) 27 IN $\mathbb{Z}_{32}$

$\gcd(27, 32)$

$= \gcd(32, 27)$

$= \gcd(27, 5)$

$= \gcd(5, 2)$

$= \gcd(2, 1)$

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 $= 1 \times 5 - 2 \times 2$

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

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

$= -13 \times 27 + 11 \times 32$

$-13 + 32 = 19$

$\boxed{MI = 19}$

5) a) $9x \equiv 11 \pmod{13}$ MI OF 9 MODULO 13 = 3

$\boxed{x = 7}$

b) $6x \equiv 3 \pmod{23}$ MI OF 6 MODULO 23 = 4

$\boxed{x = 12}$

c) $5x \equiv 9 \pmod{11}$ MI OF 5 MODULO 11 = 9

$\boxed{x = 4}$

I FOUND ALL 3 VALUES BY FINDING THE MULTIPLICATIVE INVERESE OF THE INTEGER ON THE LEFT. THEN, I MULTIPLIED BOTH SIDES BY THAT MI TO GET X BY ITSELF. I THEN DID THE RIGHT VALUE MOD BY THE VALUE GIVEN TO FIND MY X VALUE