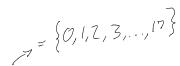
ECE 404 Homework #3

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

This homework covers topics related to finite fields.

Theory Problems

Solve the following problems.



- 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 W a group under the $gcd(\cdot)$ operation? Why or why not? (**Hint**: Find the identity element for $\{W, gcd(\cdot)\}$.)
- 4. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 27 in \mathbb{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

17+17 IS ME BIGGEST SUM POSSIBLE FROM ZIB. HEREFORE, SMCE) CLOSURE: (17+17) % 18 = 16 E Z18 11+11 10 11 15 IN BIE, ALL OTHER COMBOS WILL HAVE THE
115 SUM MOID 18 15 IN BIE, ALL OTHER COMBOS WILL HAVE THE SAME OUTCOME AND BE IN ZI8 Z18 SATISFIES CLOSURE IN MODING ADDITION

ASSOCIATIVITY:

TY:
$$[(15+10)+17] \% 18 = 12$$

$$[15+(10+17)] \% 18 = 12$$

Z18 SATISFIES ASSOCIATIVITY IN MODILO ADDITION BECAUSE -18 SMI'OU IS ACREADY ASSOCIATIVE SO THE END RESULT IS THE SAME NO MATTER THE GROUPING

IDENTITY ELEMENT:

O IS THE IDENTITY ELEMENT

AS (a+0) % 18 = a

INVERSE ELEMENT:

ELEMENT 0 1 23 4 5 0 7 8 9 10 11	17 16 15 14 13 12 11 10 9 8	ALL ELEMENTS HAVE AN INVERSE FOR MODULO ADDITION	
,			

CLOSURE: (17x17) %18 = 1 & 318

17x17 13 ME BIGGEST PRODUCT POSSIBLE FROM ZIE. MEREFORE, SINCE 1/X1/ 10 " SIE IS IN BIE, ALL OTHER COMBOS WILL HAVE THE SAME OUTCOME AND BE WZI8

Z18 SATISFIES CLOSURE IN MODING MULTIPLICATION

ASSOCIATIVITY:

[15x 10) x 17] % 18 = 12 $[15 \times (10 \times 17)]$ % 18 = 12

Z18 SATISFIES ASSOCIATIVITY IN MODULO MULTIPLICATION BECAUSE MULTIPLICATION IS ACREADY ASSOCIATIVE SO THE END RESULT IS THE SAME NO MATTER THE GROUPING

IDENTITY ELEMENT:

1 13 PAF IDENTITY ELEMENT (ax1) % 18 = 9

INVERSE ELEMENT:

NOT ALL ELEMENTS HAVE AN INVERSE

]/// 1/2 . (NOT ALL ELE	FMENTS INTO
ELEMENT 0 1 2 3 4 5	1 INVERSE	BIS FORMS A GROWF WITH MODULO ADDITION OPERATOR BUT BIS DIES NOT FORM A GROWF WITH MODULO MULTIPLICATION OPERATOR
789101123145	13	

2) gcd (30459, 27828)

gcd (27828, 8631)

gcd (8031, 1935)

gcd (1935, 891)

gcd (1891, 153)

gcd (153, 126)

gcd (126, 27)

gcd (17, 18)

gcd (18, 9)

gcd (19,0)

Jed (36459, 27828) = 9

3) THE IDENTITY IS O, SINCE gcd(a,0) = a.

THE AND WITH Gcd(a,b) = a.

ALEXAND WITH Gcd(a,b) = a.

SINCE gcd(a,0) = a.

SINCE gcd(a,0)

4) 27
$$N Z_{32}$$

$$g(d(27,32))$$

$$= g(d(32,27))$$

$$= g(d(27,5))$$

$$= g(d(5,2))$$

$$=gcd(2,1)$$

RESIDUE 27 =
$$|x27 + 0x32|$$

RESIDUE 5 = $-|x27 + |x32|$
RESIDUE 2 = $|x27 - 5x5|$
= $|x27 - 5x(-|x27 + |x32)|$
= $|x27 + 5x27 - 5x32|$
= $(x27 - 5x32)$

RESIDUE
$$1 = |x5 - 2x2|$$

 $= |x(-/x27 + /432) - 2x(0x27 - 5x32)$
 $= -/x27 + /x32 - 12x27 + lox32$
 $= -13x27 + llx32$

$$-13 + 32 = 19$$

$$/M1 = 19$$

5) a)
$$9x = 11 \pmod{13}$$
 MI OF 9 MOBULO 13 = 3
 $[x = 7]$
b) $6x = 3 \pmod{23}$ MI OF 6 MOBULO 23 = 4
 $[x = 12]$

$$5x = 9 \pmod{1}$$

$$M = 9$$

$$X = 4$$

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

BOTH SIDES BY THAT MOD BY THE VALUE GIVEN TO FIND MY X VALUE

THE RIGHT VALUE MOD BY THE VALUE GIVEN TO FIND MY X VALUE