

ECE 404 Homework #3

Due: Thursday 02/02/2023 at 5:59PM

This homework assignment will be focusing on topics related to group theory and finite fields. It involves programming as well as a part on theoretical problem-solving.

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. 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 $\{\mathbb{W}, \gcd(\cdot)\}$
3. Compute $\gcd(10946, 19838)$ using Euclid's algorithm. Show all of the steps.
4. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 19 in Z_{35} . 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) $6x \equiv 3 \pmod{23}$
 - (b) $7x \equiv 11 \pmod{13}$
 - (c) $5x \equiv 7 \pmod{11}$

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`

Submission Notes

- You must turn in a single zip file on Brightspace with the following naming convention: `HW03_<last_name>_<first_name>.zip` . Do not turn in files other than those listed below. Your submission must include:
 - A PDF *containing your answers to the theory problems. You are allowed to include scans or photos of handwritten work in the PDF, but your work must be clearly legible.*
 - The file `mult_inv.py` containing your code for the programming problem.