ECE 404 Homework #3

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

This homework is on topics related to finite fields.

IMPORTANT: For this homework, you will have both a **physical** (i.e. paper hard-copy) and **electronic** submission. The physical submission should be handed in at the front of the classroom on the due date. See the Submission Notes section for details.

Theory Problems

Solve the following problems.

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.
2. Compute gcd(29495, 16983) using Euclid's algorithm. Show all the steps.
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 $\gcd(a,b)$).
4. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 25 in Z_{28} . 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 using brute-force methods:
   (a) 8x $\equiv$ 11 (mod 13)
   (b) 5x $\equiv$ 3 (mod 21)
   (c) 8x $\equiv$ 9 (mod 7)

Programming Problem

1. Write a program that takes as input a small integer n (say, smaller than 50) and determines if Z_n 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".

Submission Notes

- The paper (hard-copy) submission must include your answers to the theory problems as well as a printout of your program.
- For the electronic submission, you must turn in only the file containing your program (e.g. a .py file). below. .

Electronic Turn-in

`turnin -c ece404 -p hw03 Fields.pl` (if using Perl)
`turnin -c ece404 -p hw03 Fields.py` (if using Python)