Homework 5: Number Theory

Submission policy. Submit your answers on Blackboard by 11:59pm Friday, **Nov. 5**, 2021. Your submission should include a .PDF file with all the answers to the theoretical problems. You should try to typeset your homeworks. Latex is especially recommended. No late submissions will be accepted. Your writeup MUST include the following information:

1. Your name and whether you take the class at **487** or **587** level.
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

The homework will be graded by the class TA Anuj Pokhrel (apokhre@gmu.edu).

Exercise 1. Abelian Groups [10 points] Is the group $\{0,1\}^n$ (i.e binary strings of length n) under XOR operation an abelian group? (Argue for each one of the properties seperately to receive full points).

Exercise 2. Euclidean Algorithm [30 points] Write down your G number, take the first 6 digits (after the 0) and split them into two 3 digit numbers a and b, i.e. if your G number is G01043714 then set $a = 104$ and $b = 371$.

1. "Run" the Euclidean algorithm for your values a and b and return $gcd(a, b)$. For your answer read Algorithm B.7 from textbook (page 551) and explicitly write down your computations as steps of the algorithm.
2. Do the same for the extended Euclidean algorithm (Algorithm B.10 from textbook), explain all steps and return values X and Y.

Exercise 3. [10 points] Calculate by hand the value 3^{1500} mod 100 using Algorithm B.13 from the textbook. Make sure to explain the steps.

Exercise 4. Cyclic Groups 1 [20 points] Consider the group Z_{15} (group under addition modulo 15).

- Write down all the elements of the group.
- What is the order of the group?
- Compute the inverse for each element of the group.

- Is the group cyclic?

Exercise 5. Cyclic Groups 2 [20 points] Consider the group Z_{15}^* (invertible elements modulo 15 under multiplication modulo 15).

- Write down all the elements of the group.
- What is the order of the group?
- Compute the inverse for each element of the group.
- Is the group cyclic?

Exercise 6. [10 points]
Compute $\phi(N)$ (i.e. the number of invertible elements modulo N) in the following cases:

- $\mathbb{Z}_{10}$
- $\mathbb{Z}_{10}^*$
- $\mathbb{Z}_{251}$