EE 720: Introduction to Number Theory and Cryptography (Spring 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 4: 10 points Date: March 24, 2019

Upload the solutions as a **pdf** file in Moodle. You can upload a scanned version of your handwritten solution. The **upload deadline** will be 11:00pm IST on Sunday, March 31, 2019.

1. [2 points] Prove that every cyclic group G of order n is isomorphic to $\mathbb{Z}_n$ with addition modulo n as the operation.

2. [2 points] Prove that every cyclic group is abelian.

3. [2 points] Using the Chinese remainder theorem, find x modulo 105 which satisfies the following congruences.

$$x = 1 \bmod 3$$
$$x = 2 \bmod 5$$
$$x = 3 \bmod 7$$

   Note: This can be solved using brute force. But I want you to use the relation $x = a_1 M_1 y_1 + \cdots + a_l M_l p_l$ where $M = p_1 p_2 \cdots p_l$, $M_i = \frac{M}{p_i}$, and $M_i y_i = 1 \bmod p_i$. See lecture 18 outline.

4. [2 points] For an integer $e \geq 1$ and prime p, prove that $\phi(p^e) = p^e \left(1 - \frac{1}{p}\right)$.

5. [2 points] For any integer $n > 1$ with prime power factorization $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1 \geq 1, e_2 \geq 1, \ldots, e_k \geq 1$, prove that

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

   ***Hint**: Use the Chinese remainder theorem and the result from question 4.*