CS5319 Advanced Discrete Structure

Exam 3 – January 11, 2022 (13:20–15:10)

You may assume that all properties about divisibility, gcd, modulo arithmetic, Φ function, and results like Fermat's theorem, Wilson's theorem, Euler's theorem, Lagrange theorem, Chinese Remainder Theorem, etc, discussed in the class, in the tutorials, or in the homework are correct.

Answer all five questions. Total marks = 100.

1. Let Q^+ denote the set of positive rational numbers.

   (15%) Is the algebraic system $(Q^+, \times)$ a group, where $\times$ denotes the usual multiplication operator? Justify your answer.

2. (15%) Find the last two digits of 53^{723} without a calculator. Show your steps, and justify your answer.

3. (35%) Using RSA with key $(e, n) = (101, 779)$, we obtain the following ciphertext

   $$299 \quad 656 \quad 280 \quad 47 \quad 216$$

   (a) (10%) Apply the extended Euclidean algorithm to find the private key d.

   (b) (20%) What is the original plaintext? Write five numbers as your answer.
   Note: You may write a program to help the computation.

   (c) (5%) Assume that in the original plaintext, we use the numbers [27, 52] to represent the English characters [a, z]:

   $$\mathtt{a} = 27, \quad \mathtt{b} = 28, \quad \mathtt{c} = 29, \quad \mathtt{d} = 30, \quad \ldots, \quad \mathtt{y} = 51, \quad \mathtt{z} = 52.$$

   What is the original plaintext?

4. Consider coloring a regular hexagon (6-sided polygon) on a plane where each vertex can be colored in black or white, and each edge can be colored in red, green, or blue.

   Two colorings are the same if one can be obtained from the other by rotating the hexagon on the plane.

   (20%) How many distinct colorings are there? Justify your answer.

5. Long time ago, we have studied the Catalan number C_n, which is an integer whose value is equal to:

   $$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

   (15%) Let p be a prime number greater than 2. When C_p is divided by p, what will be the remainder? Express the remainder in its simplest form, and justify your answer. Give reasons for each claim you make.