COL759 Tutorial 2

September 2024

Instructions

- Do not copy from GPT, your friends, or any other internet resources.
- Understand the algorithms and work through the mathematical steps manually, and include all the steps in the solution.
- You are supposed to write the solution on paper or in LaTeX, as per your preference, and then submit the final PDF in Gradescope.

Problem 1: Find factors of 1649 using Pollard's Rho Method **(20 Marks)**

Problem 2: Factorization of $N = 1000000000039$ Using the Quadratic Sieve Method . Find all the factors of N, write down the the steps in the solution. **(35 Marks)**

Problem 3: Baby-Step Giant-Step Algorithm **(15 Marks)**
The Baby-Step Giant-Step algorithm is used to solve the discrete logarithm problem efficiently. In this case, we need to find x such that:

$$7^x \equiv 512 \mod 1093$$

Problem 4: Pollard's Rho Algorithm for Discrete Logarithms (30 Marks)
You are tasked with finding x such that:

$$5^x \equiv 89 \mod 383$$