Assignment-I

Programming Assignments on Number Theoretic Algorithms

Submission Deadline: 22nd September, 2022

Note: For all the programs, users should be able to enter the input. Based on the input, the program returns the output. If the user's input is not in the desired form, the program should return $\perp$. (For example, if the user enters character or fractional number in the Euclidean algorithm, the algorithm will return $\perp$)

1. Implement the Euclidean Algorithm that will take two inputs a and b such that $b > 0$ and will return the greatest common divisor of a and b. Also plot the time curve of the Euclidean Algorithm with respect to different inputs.

2. Given a positive integer N and $a \in \mathbb{Z}_N$, write a program that will take input N and $a \in \mathbb{Z}_N$, and determine whether $a \in \mathbb{Z}_N^*$ or not. If it is, then the program should also return the multiplicative inverse of a modulo N.

3. Given a positive integer N, $a \in \mathbb{Z}_N$ and $b > 0$, write a program (recursive and iterative) that will take input $N, a \in \mathbb{Z}_N$, and $b > 0$ and return $a^b \mod N$. Compare the time required in the trivial algorithm and in the square and multiplication algorithm through graphical plots

4. Write a program that will take an input n and N such that $n = \|N\|$ and return an element $a \in \mathbb{Z}_N^*$ which should be uniformly sampled from $\mathbb{Z}_N^*$.

5. Write a program that will take an input n. The program will randomly sample a prime number p of length n, which will define a cyclic group $\mathbb{Z}_p$. Then the program should return a randomly sampled element which is a generator of $\mathbb{Z}_p$.