KING SAUD UNIVERSITY

COLLEGE OF COMPUTER & INFORMATION SCIENCES
DEPT OF COMPUTER SCIENCE

CSC281 Discrete Mathematics for Computer Science Students
Third Semester 1444 AH
Due: TBA
Instructor: Prof Aqil Azmi

Group Term Project

The goal of this project is to develop an algorithm that can efficiently find all the primitive roots modulo *n*. A primitive root, also known as a generator, is an integer that generates all the elements in the set of residues modulo *n* when raised to various powers.

The algorithm will take an input value *n*, which represents the modulus, and it will search for a primitive root within the range of 1 to $n-1$. The algorithm will systematically check each number in this range to determine if it satisfies the primitive root property.

To determine if a number *g* is a primitive root modulo *n*, the algorithm will iterate over all the values from 1 to $n-1$ and compute *g* raised to the power of each value modulo *n*. If all the results are unique and cover all the residues modulo *n*, then *g* is a primitive root.

For example, for *n* = 7, one primitive root module 7 is 3. The algorithm will check each number from 1 to 6 to find a primitive root. The algorithm will determine that 3 is a primitive root because when raised to the powers 1, 2, 3, 4, 5, and 6, the resulting values modulo 7 are unique and cover all the residues modulo 7. In fact, 5 is another primitive root module 7. Another example. For input n = 11, we have four different primitive roots module 11, namely: 2, 6, 7, 8.

The success of the project will be measured by the correctness and efficiency of the algorithm in finding primitive roots modulo *n* for various values of *n*. Overall, this project aims to provide a reliable and efficient solution for finding all the primitive roots modulo *n*, which can be utilized in various applications involving modular arithmetic, cryptography, and number theory.

Instructions

This is a group project. Each pair of students will work as a team. You are free to use any convenient programming language. This project is worth 15 points.

What to submit

(a) Cover sheet with your names and a signed pledge.
(b) Write-up of the project (a brief description of your algorithm; the data structure used; cost analysis; sample runs and the conclusion).
(c) Hardcopy of your source code and report on Flash memory or CD with source and executable.