Alexandria University
Faculty of Engineering
Computer and Systems Engineering
Department

CS211 Mathematics for Computer Science
Assigned: Sunday, November 24^{th}, 2019
Due: Tuesday, December 3^{rd}, 2019

Assignment
Number Theory

1 Question 1: Fast Exponentiation

- Implement the following procedures and compare the execution time of each with the increase of number of bits representing an integer. Also report on when the procedure breaks (overflow).
- Implement it in 4 versions. The following two naïve versions, in addition to, fast exponentiation in iterative and recursive versions.

Naïve 1

```
c =1
for i = 1 to b
c = c * a
c= c mod m
return c
```

Naïve 2

```
c= 1
for i = 1 to b
c = (c * a) mod m
return c
```

2 Question 2: Extended Euclidean Algorithm

Input: a, b
Output: d = gcd(a,b) and s, t such that d = s.a + t.b

3 Question 3: Chinese Remainder Theorem

Input: m_1,m_2,.....,m_n($M = m_1.m_2.....mn$), A,B $\in Z_M$
Output: C = A+B, D = A * B
Implement the addition and multiplication in both the domain Z_M and the domain $Z_{m1} * Z_{m2} * \ldots * Z_{mn}$. Compare the execution time of both version with the increase of the number of bits representing the integers in Z_M.

4 Question 4: Prime Number Generation

Implement a prime number generation procedure and show its execution time in terms of the number of bits representing an integer.

5 Delivery Requirements

- A detailed report is required, it should contain
  - Problem statement
  - Used data structures
  - Algorithms used documented using flow charts or pseudo code
  - Assumptions and details, you find necessary to be clarified
  - Any design decisions
  - Sample runs
- Take care about the following
  - Code comments
  - Naming conventions
  - Code organization
- You have to work **individually**.
- You should send your report by email to: *fadynabilyacoub@gmail.com* with subject: **DiscreteAssignment2 [Name1 id]**
- No late submissions are allowed.
- **Make sure you provide a clear and detailed report**