***Assignment***

***Number Theory***

**First student**

Name : Mahmoud Ebrahim Elsayed Mahmoud

Id : 58

**Second student**

Name : Hamza Hassan

Id : 26

1. **Problem statement.**
2. **Used data structures.**
3. **Algorithms used documented using pseudo code.**
4. **Sample runs.**
5. **Problem statement.**
6. 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 version, 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

1. Question 2: Extended Euclidean Algorithm

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

1. Question 3: Chinese Remainder Theorem

* Input: m1,m2,……..,mn(M = m1.m2…..mn), A,B M
* Output: C = A+B, D = A \* B
* Implement the addition and multiplication in both the domain ZM and the domain Zm1 \* Zm2 \* ………. \* Zmn. Compare the execution time of both version with the increase of the number of bits representing the integers in ZM.

1. Question 4: Prime Number Generation

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