Lab Assignment – 1 (10 Marks)

Execute the following programs using gmp library in C or Python.

Note: Do not use predefined functions from any Library or Header file, whenever it is possible. Instead write your own function for it.

Abbreviation: HAC- Handbook of Applied Cryptography

Sno.	Program	Reference, if any
1.	[Common divisors] Given n, $\{m_i\}_{i=1}^{n}$ integers, print all common divisors of $(m_1, m_2, \dots, m_n)$.	
2.	Extended Euclidean algorithm to output x, y when a, b is given, such $ax + by = gcd(a, b)$	Notes or Algo 2.107 HAC
3.	[Fundamental Theorem of Arithmetic] Given any integer output the product of primes, in ascending order.	Notes
4.	[Reduced Residue System Modulo m] Given an integer m, output the RRSM_m set of integers. And also output the value of $\varphi(m)$	Notes
5.	Given a, x and n, output $a^x (mod\ n)$. Use fermat theorem concept. Also print intermediate equations while computing, in any readable form.	Algo 2.143 HAC
6.	Given a and m, first print whether multiplicative inverse of $a\ (mod\ m)$ exist Y/N then output its inverse, if exist.	Algo 2.142 HAC
7.	[Solutions of congruence] Given a, b and m, print whether solution to the congruence $ax \equiv b(mod m)$ exist Y/N. If Yes then output the number of solutions and all the solutions.	
8.	[Solution to system of congruences] Given set of integers $\{(a_i, b_i, m_i)\}_{i=1}^{n}$, print whether there exist common solution x which satisfy the system of congruences of the form $a_i x \equiv b_i\ (mod\ m_i)$. If exist then print all the solutions. Use user defined CRT function.	Notes or Algo 14.71 HAC
9.	[Order] Given a and m, print order of a under modulo m.	Notes
10.	[Primitive roots] Given m, print the total number of primitive roots exist and print all the primitive roots, under modulo m.	Notes

Instructions:

All programs should be name as prgi.c or prgi.py, if it is program 1 then prg1.c or prg1.py

All input to the program should be command line input. We test it using command line input only. For example, for prg2.c say its executable file name is prg2 then we test as,

$prg2 5 7 <enter>

Where $ is command prompt, a = 5 and b = 7, as per prg2.c question.

And print only exact output (without any English sentences). Because we store output in a text file using linux command, such as $prg2 5 7 >> out.txt <enter>

We also do plagiarism test of each program, if percentage of similarity is higher then marks will not be given. Percentage fixation will be discuss with you later.