Assignment #1

Divisibility

1) Please implement the “Euclid’s Extended Algorithm” to calculate GCD, multiplicative inverse and to check the relatively prime condition.
    - What happens to your program if b=0? Fix the program so that it deals with case correctly.
    - Please design your code in modular form which can be called to calculate multiplicative inverse of a number for mod p or only to calculate the GCD of two numbers etc..
2) Please implement Chinese Remainder Theorem to solve x value for the given multiple congruencies with created modules at (1).
3) Please implement given Primality Testing algorithm.

Notes:

- You can write your code in C or Java.
- Please note that these modules will be used for the following assignments to build cryptosystems.
- Please try to build your code for multi-precision (big) integer numbers.
- Please prepare a short report about your implementation environment and explanations for your code, your experiments and add some screen shots about selected example executions for each module.
- Submit the report, source and executable object code of your assignment under one compressed file (Cng471-StudentName-Surname-Hw1.zip).
- The last submission date for this assignment: Apr. 15, 2018 Sunday, until 22:00.

Thank you.

Serap