EXTENDED EUCLIDEAN ALGORITHM IMPLEMENTATION

1) Using any programming language of your choice implement the Extended Euclidean algorithm **[20 Marks]**

2) **Specifications:** The program should take two inputs 1) An integer ***a,*** which is the modulus 2) A non-negative integer ***b*** that is less than ***a***. The program should output three values 1) ***gcd(a,b)*** 2) Integer ***x*** and 3) Integer ***y,*** such that ***ax + by = gcd(a,b)***

Test 1 [5 Marks]

1) Run your program with ***a = 1759 b = 550***

2) What are your outputs?

3) What is the modular multiplicative inverse of ***550 mod 1759***?

Test 2 [5 Marks]

1) Run your program with ***a = 43 b = 17***

2) What are your outputs?

3) What is the modular multiplicative inverse of ***17 mod 43***? Note that the modular multiplicative inverse has to be non-negative and less than 43.

Test 3 [5 Marks]

1) Run your program with ***a = 400 b = 10***

2) What are your outputs?

3) What is the modular multiplicative inverse of ***10 mod 400***? Be mindful of the gcd value to answer this question

Submission

1) Submit the following documents separately in CANVAS by the deadline. **NO ZIPPED FILES ALLOWED**

1) All your code files

2) A detailed **README** file, which should explain how to run the code with sample input and output. If you are unfamiliar with READMEs you can find an introduction here https://www.makeareadme.com/ , here https://medium.com/@meakaakka/a-beginners-guide-to-writing-a-kickass-readme-7ac01da88ab3 and here https://www.youtube.com/watch?v=RZ5vduluea4. Note that the README file you

submit for this project need not be complex, it only needs to at least explain how to compile the code and run the code with examples. **[5 marks]**

3) Your executable file and your **DOCKER** file. Please see the file **DOCKER INSTRUCTIONS** for information on how to create your docker file.**[10 marks]**

4) A report (which should include your answer to the test results with screen shots)

5) Note that your submission will be checked for plagiarism. All submissions with verified plagiarism cases will graded 0