Comp 2700 (Discrete Structures) Fall 2019. Programming Assignment 1.

Submissions: This assignment is due at 11:59 PM on the 21st of Nov, 2019. Each student must submit his or her own assignment. This is a programming assignment. You have to submit code that can be run on a computer. You can use Java, C, C++ or Python to write code. In any case, your submission should be a single file (don't compress it) containing your code (not compiled code), any relevant instructions to compile or run your code as comments. The input/output format for each problem is specified with the problem. For the input format, you may assume the format will be absolutely as specified, i.e., you do not need to check for errors in the input format. For the output, your code must output its results on the standard output in the strict format desired of it (and nothing else).

Academic Integrity: You are encouraged to work in groups, but everyone must write his/her own code. Absolutely no copying is allowed. Please refer to the course policies and schedules about this. If you have worked with other students on the assignment or referred to external sources, please mention all names and sources on your assignment.

Problem 1[50 pts]: Write a program that prompts the user to enter two positive integers named a and b. Then, output the Bezout coefficients of a, b. Recall that the Bezout coefficients are (any) integers s, t such that:

$as + bt = \gcd(a, b)$.

Problem 2[50 pts]: Write a program that prompts the user to enter three positive integers a, b, n. Then, output the general form of solutions to the congruence equation $ax \equiv b \pmod{n}$ if there is such a solution. If there is no solution output "NO SOLUTION".

For example, suppose I enter $a = 2, b = 3, n = 6$ the output should be "NO SOLUTION". If on the other hand, I enter $a = 2, b = 4, n = 6$ then the general solution is $x \equiv 2 \pmod{3}$ so your program outputs $x = 2 \pmod{3}$.

Hint: Recall that we have seen how to solve congruences like $ax \equiv b \pmod{n}$ *if* $\gcd(a, n) = 1$*. Clearly you can check if* $\gcd(a, n) = 1$ *and if so you know what to do. If that is not the case however, then first show that the equation has a solution iff* $d|b$ *where* $d = \gcd(a, n)$ *and in this case it is enough to solve the equation* $(a/d) \equiv (b/d) \pmod{(n/d)}$*. Also convince yourself why* $\gcd(a/d, n/d) = 1$*. Now use how to solve congruences of the type you have seen in class.*