Name: ______________________

Entry number: ______________________

There are 3 questions for a total of 10 points.

---

1. Recall the `Extended-Euclid-GCD` algorithm discussed in class for finding the gcd of positive integers $a \geq b > 0$ and integers x, y such that $ax + by = gcd(a, b)$. The algorithm makes a sequence of recursive calls until the second input becomes 0. For example, the sequence of recursive calls along with the function-call returns for inputs $(2, 1)$ are:

$$\overset{(1,0,1)}{\leftarrow} \texttt{Extended-Euclid-GCD}(2,1) \overset{\overset{(1,1,0)}{\leftarrow}}{\rightarrow} \texttt{Extended-Euclid-GCD}(1,0)$$

   (a) (1 ½ points) Write down the sequence of recursive calls along with function-call returns that are made when the algorithms is executed with inputs $(995, 53)$.

Solution: $\overset{(1,22,-413)}{\leftarrow}$ `Extended-Euclid-GCD`$(995, 53)$ $\overset{\overset{(1,-17,22)}{\leftarrow}}{\rightarrow}$ `Extended-Euclid-GCD`$(53, 41)$ $\overset{\overset{(1,5,-17)}{\leftarrow}}{\rightarrow}$ `Extended-Euclid-GCD`$(41, 12)$ $\overset{\overset{(1,-2,5)}{\leftarrow}}{\rightarrow}$ `Extended-Euclid-GCD`$(12, 5)$ $\overset{\overset{(1,1,-2)}{\leftarrow}}{\rightarrow}$ `Extended-Euclid-GCD`$(5, 2)$ $\overset{\overset{(1,0,1)}{\leftarrow}}{\rightarrow}$ `Extended-Euclid-GCD`$(2, 1)$ $\overset{\overset{(1,1,0)}{\leftarrow}}{\rightarrow}$ `Extended-Euclid-GCD`$(1, 0)$

   (b) (½ point) What is the inverse of 53 modulo 995? That is, give a positive integer x such that $53 \cdot x \equiv 1 \ (mod\ 995)$. Write "not applicable" in case no such integer exists.

(b) **582**

2. State true or false with reasons:

   (a) (1 point) For all positive integers $a \geq b > 0$ there exists *unique* integers x, y such that $ax + by = gcd(a, b)$.

(a) **False**

Solution: We give a counterexample. Consider $a = 5$ and $b = 3$. We have $2 \cdot 5 + (-3) \cdot 3 = 1 = 5 \cdot 5 + (-8) \cdot 3$.

   (b) (1 point) Let $m > 2$ be a prime number and let $1 < a < m$ be any integer. Then a has a unique inverse with respect to the operation multiplication modulo m. That is, there is a unique integer $1 < b < m$ such that $ab \equiv 1 \ (mod\ m)$.

(b) **True**

Solution: For the sake of contradiction let there be two inverses $1 < b < c < m$ of a. Then we have:

$$\begin{aligned} b &\equiv (b \cdot (ac))\ (mod\ m) \\ &\equiv ((ba) \cdot c)\ (mod\ m) \\ &\equiv c\ (mod\ m). \end{aligned}$$

This is a contradiction. So the inverse of any $1 < a < m$ is unique with respect to multiplication modulo m.

3. Consider one of the problems in the tutorial sheet related to the possible way of leaving a certain amount of water given two jugs with integer capacities S and L. Recall that you have unlimited source of water and nothing but the two given jugs. Answer the following questions:

   (a) (3 points) Design an algorithm that takes as input three positive integers S, L, and B such that $B < S < L$ and outputs "Not Possible" if it is not possible to leave B litres of water in any of the two jugs and otherwise it outputs the precise way to make sure that one of the jugs has exactly B litres of water.

   Solution: Here is the pseudocode for the algorithm.
   `JugProblem`(S, L, B)
   - $(d, x, y) \leftarrow$ `ExtendedEuclidGCD`(L, S)
   - If(d does not divide B) return ("Not possible")
   - Compute q such that $B = dq$
   - If $(x > 0)$ return("Fill the smaller jug qx times and keep emptying in the larger jug. Whenever the larger jug becomes full, it is emptied.")
   - else return("Fill the larger jug qy times and keep emptying in the smaller jug. Whenever the smaller jug becomes full, it is emptied.")

   (b) (1 point) Execute your algorithm for input $S = 15, L = 21, B = 12$ and write the output below.

   Solution: Fill the smaller jug 12 times and keep emptying in the larger jug. Whenever the larger jug becomes full, it is emptied.

   (c) (1 point) Execute your algorithm for input $S = 5, L = 8, B = 3$ and write the output below.

   Solution: Fill the larger jug 6 times and keep emptying in the smaller jug. Whenever the smaller jug becomes full, it is emptied.

   (d) (1 point) Execute your algorithm for input $S = 21, L = 33, B = 16$ and write the output below.

   Solution: Not possible.