

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:

$$\stackrel{(1,0,1)}{\longleftarrow} \text{Extended-Euclid-GCD}(2, 1) \stackrel{(1,1,0)}{\longrightarrow} \text{Extended-Euclid-GCD}(1, 0)$$

- (a) (1 $\frac{1}{2}$ points) Write down the sequence of recursive calls along with function-call returns that are made when the algorithms is executed with inputs $(985, 53)$.

- (b) ($\frac{1}{2}$ point) What is the inverse of 53 modulo 985? That is, give a positive integer x such that $53 \cdot x \equiv 1 \pmod{985}$. Write “not applicable” in case no such integer exists.

(b) _____

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) _____

- (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 $ab \equiv 1 \pmod{m}$.

(b) _____

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.
- (b) (1 point) Execute your algorithm for input $S = 18, L = 21, B = 12$ and write the output below.
- (c) (1 point) Execute your algorithm for input $S = 13, L = 21, B = 3$ and write the output below.
- (d) (1 point) Execute your algorithm for input $S = 21, L = 39, B = 16$ and write the output below.