PROBLEM SET 7

Anthony Tam, CSC236 11/11/2016

Question 1: Analyze the LCD function.

ANSWER: Part a)

$Inv(x, y) : x > 0 \wedge x \leq LCM(a, b) \wedge LCM(x, y) = LCM(a, b)$

ANSWER: Part b)

Base Case:

When the loop is reached, x = a and y = b.

$x > 0$ holds since by definition $x \geq 1$

$x \leq LCM(a, b)$ holds since the LCM must either be on of the terms or will always be a greater multiple of the terms.

$LCM(a, b) = LCM(a, b)$

$\therefore$ the base case holds.

Inductive Step:

We will assume the invariant and the loop guard currently hold:

$Inv(x_0, y_0) : x_0 > 0 \wedge x_0 \leq LCM(a, b) \wedge LCM(x_0, y_0) = LCM(a, b)$

$x_0 \neq y_0$

We will prove the following:

$Inv(x_1, y_1) : x_1 > 0 \wedge x_1 \leq LCM(a, b) \wedge LCM(x_1, y_1) = LCM(a, b)$

Case One ($x_0 < y_0$):

$x_1 = x_0 + a$

$y_1 = y_0$

$x_1 \% a = 0$ (x_1 is a multiple of a)

This means $LCM(x_1, y_1) = LCM(x_0, y_0) = LCM(a, b)$

Since a is a positive natural number, $x_1 > 0$

x_1 has either yet to reach the LCM or is equal to it, $x_1 \leq LCM(a, b)$.

Case Two ($x_0 > y_0$):

$x_1 = x_0$

$y_1 = y_0 + b$

$y_1 \% b = 0$ (y_1 is a multiple of b)

This means $LCM(x_1, y_1) = LCM(x_0, y_0) = LCM(a, b)$

Since b is a positive natural number, $y_1 > 0$

y_1 has either yet to reach the LCM or is equal to it, $y_1 \leq LCM(a, b)$.

This concludes the inductive case.

ANSWER: Part c)

The invariant states that $LCM(x, y) = LCM(a, b)$
When the loop terminated, x and y will be equal to each other meaning that it is the LCM. The value of x will be returned, an integer representing the LCM between a and b. This satisfies the post condition.

ANSWER: Part d)

The variant will be $Max(x, y) - Min(x, y)$ since x and y will continue to increase, the difference between them will approach 0. However, sometimes x increases in the loop and sometimes y will increase. To account for this we will ensure we subtract the higher value from the lower one.

By looking at the invariant, we know the x and y values will both approach the LCM of each other. This means the variables are going to become equal. At this point the loop will break and the variant will be true.

Question Two: Find a variant for the mystery function

The variant $a + b$ is not a suitable variant since on iterations of the loop which fall under case 1, the value of $a + b$ will not change. Since it does not decrease after each iteration, it does not follow the definition of a variant.
A more suitable variant is $((b + 1) \cdot (a + 2)) - 1$
By adding 1 to the "a" term and 2 to the "b" term, we will ensure that each iteration of the loop causes a change in the multiplication. When If the loop falls under case 2, the addition to the a term is reduced to 1, otherwise 2 is added to the term. A minimum of 1 must be added to each term to counteract the possible 0 or negative value when running the algorithm. Lastly subtracting 1 at the end will ensure that the variant ends at 0, breaking the loop.