Zackery Field
ID: 23031734
CS 70, Summer 2013
Homework 2
Problem 4 [10 Points]

1. [10 Points] Application of the extended Euclidean algorithm to find linear combinations.

   (a) [5 Points] Use the algorithm to compute GCD(4725, 273) and express GCD(4725, 273) as $a * 4725 + b * 273$, for some integers a,b. Show all steps of the algorithm.
   Finding the GCD:

$$\begin{aligned} 4725 &= 17 * 273 + 84 \\ 273 &= 3 * 84 + 21 \\ 84 &= 4 * 21 \\ GCD &= 21 \end{aligned}$$

   Forming $GCD = a * x + b * y$:

$$\begin{aligned} 21 &= 273 - 3 * 84 \\ &= 273 - 3(4725 - 17 * 273) \\ &= -3 * 4725 + 52 * 273 \\ a &= -3 \\ b &= 52 \end{aligned}$$

   $21 = (-3 * 4725) + (52 * 273)$

   (b) [5 Points] Prove that for all $x > 0$ and $y > 0$, $GCD(x, y)$ is the smallest positive number that can be written as an integer linear combination of x and y.

   Proof by contradiction:

   Assume that there is a smaller positive number than $GCD(x, y)$ that can be written as a linear combination of x and y. Let $sx + ty < GCD(x, y)$, and $t > 0$, describe the assumed integer linear combination.

$$\begin{aligned} sx + ty &< GCD(x, y) \\ \frac{sx + ty}{GCD(x, y)} &< 1 \\ s\frac{x}{GCD(x, y)} + t\frac{y}{GCD(x, y)} &< 1 \\ sq + tr &< 1, where: \{q, r\} \in \mathbb{Z} \end{aligned}$$

$q \geq 1$and $r \geq 1$. Taking the least case, where $\{q, r\} = 1$, then we confirm $s + t < 1$. So $0 < t < 1$and $0 < s < 1$, a contradiction since we assumed that $sx + ty$ was a positive integer linear combination of x and y.