Homework 2

CSE/MATH 467 Due: 02 September, 2016

1. Preview Problem from HW1. Implement the script which is Bressoud's Alogrithm 1.7 (Algorithm 1 in our pseudocode available at `http:/www.math.psu.edu/wdb/467/pseudocode.pdf`) and test it on the following pairs of numbers:

- 34 126, 2718
- 21 377 104, 12 673 234
- 355 876 536, 319 256 544
- 84187 85375, 78499 11069

In particular you should define a function and then evaluate the function on the pairs given above. Do not use a screen prompt. In your final project, you will have various functions calling up and using values of other functions, and requiring prompts for the interior functions would be worse than useless.
What to hand in: Print out your script and print out a record of the session showing how you initialize the script and evaluate the function it defines on the given pairs.

2. One formulation of the Principle of Mathematical Induction is the following:

Every non-empty set of positive integers has a least element.

Use this formulation to prove the validity of the
Division Algorithm for positive integers. If $a \in \mathbb{Z}_{\geq 0}$ and $b \in \mathbb{N}$, then there exist $q, r \in \mathbb{Z}_{\geq 0}$ with

$$a = b \cdot q + r \qquad 0 \leq r < b.$$

3. [Based on Bressoud 1.09] a) Using the Euclidean Algorithm and hand calculation, find $\gcd(34126, 2718)$.
b) Use the calculation of the first part to express $\gcd(34126, 2718)$ as an integral linear combination of 34126 and 2718.

4. [Bressoud 1.19]
   a) Find integers m, n such that

$$1947 \times m + 264 \times n = 33.$$

   b) For arbitrary $a, b \in \mathbb{Z}$, show how to always find infinitely many $k, l \in \mathbb{Z}$, depending on a, b with $ka + lb = 0$.
   c) Show that there are infinitely many integral solutions of

$$1947 \times m + 264 \times n = 33.$$

This illustrates that the coefficients produced by the Euclidean Algorithm are far from being the only ones giving a linear combination equal to $\gcd(a, b)$.

5. a) Let $x, y \in \mathbb{Z}$ not both be zero. We have used in the class the principle that, for any $a, b \in \mathbb{Z}$, $\gcd(x, y) \mid ax + by$. Give that proof here again.
b) Deduce that for any $a, b, c, d \in \mathbb{Z}$, since similarly $\gcd(x, y) \mid cx + dy$, we must have that $\gcd(x, y) \mid \gcd(ax + by, cx + dy)$.
c) Finally conclude that if, in addition, $ad - bc = \pm 1$, then

$$\gcd(x, y) = \gcd(ax + by, cx + dy).$$

The fact that $\gcd(x, y) = \gcd(x + ky, y)$ that we used for the Euclidean Algorithm is a very special case of this exercise.
Hint: Recall from linear algebra that under these conditions the linear map

$$\begin{pmatrix} x \\ y \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

is invertible. What is the inverse matrix and what does that say about the vector $\begin{pmatrix} x \\ y \end{pmatrix}$ in terms of $\begin{pmatrix} x' \\ y' \end{pmatrix}$?