ESP Math 294 **Fall 2018**

Worksheet 11

Week of 5 November 2018

Greatest common divisor (GCD) of $a, b \in \mathbf{Z}$: the largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$.
Least common multiple (LCM) of $a, b \in \mathbf{Z}$: the smallest $m \in \mathbf{Z}$ such that $a \mid m$ and $b \mid m$.

Recall the **Euclidean algorithm**, which finds the GCD of $a, b \in \mathbf{Z}$.

put in a, b, find $q_0, r_0 \in \mathbf{Z}$	$a = q_0 b + r_0$	$0 \leqslant r_0 < \lvert b\rvert$
move b, r_0, find $q_1, r_1 \in \mathbf{Z}$	$b = q_1 r_0 + r_1$	$0 \leqslant r_1 < \lvert r_0\rvert$
move r_0, r_1, find $q_2, r_2 \in \mathbf{Z}$	$r_0 = q_2 r_1 + r_2$	$0 \leqslant r_2 < \lvert r_1\rvert$
move r_1, r_2, find $q_3, r_3 \in \mathbf{Z}$	$r_1 = q_3 r_2 + r_3$	$0 \leqslant r_3 < \lvert r_2\rvert$
	$\vdots$	
	$r_{n-2} = q_n r_{n-1} + r_n$	$0 \leqslant r_n < \lvert r_{n-1}\rvert$
	$r_{n-1} = q_{n+1} r_n + 0$	

Then r_n is the GCD of a and b. By substituting back all the r_i for $i < n$, we can find a **linear combination** $ax + by = r_n$ relating a, b, and their GCD. Moreover:

$$\textit{There exist integers } x, y \textit{ such that } ax + by = 1 \quad \Longleftrightarrow \quad \gcd(a, b) = 1.$$

---

1. Do not use a calculator for the following questions.
   (a) Compute the GCD of 403 and 187 by the Euclidean algorithm.
   (b) Compute the GCD of 2233 and −455 by the Euclidean algorithm.
   (c) Write each of the answers from parts (a) and (b) as linear combinations of the respective pairs of numbers.

2. Find all integer solutions to the equation $40x + 25y = 600$.
   Hint: Use the Euclidean algorithm on the coefficients to find one solution, then generalize.

3. What combinations of 18-cent and 33-cent stamps can be used to mail a package which requires a postage of 6 dollars?

4. Recall that $|a \cdot b| = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$. Find all the pairs of positive integers $a \leqslant b$ such that $\gcd(a, b) = 60$ and $\operatorname{lcm}(a, b) = 4200$.

5. For all $a, b, c \in \mathbf{Z}$ with $c > 0$, prove that $\gcd(ac, bc) = c \gcd(a, b)$.

6. For all positive $a, b \in \mathbf{Z}$, prove that $a \mid b$ if and only if $a^2 \mid b^2$.