Homework 4: Due Wednesday, February 12

Problem 1: Show that for all $a \in \mathbb{Z}$, either there exists $k \in \mathbb{Z}$ with $a^2 = 3k$ or there exists $k \in \mathbb{Z}$ with $a^2 = 3k + 1$. In other words, show that for all $a \in \mathbb{Z}$, the unique remainder upon dividing a^2 by 3 is always either 0 or 1.
Hint: Start by performing division with remainder on a.

Problem 2: Use the Euclidean Algorithm to find the greatest common divisor of the following pairs of numbers a and b. Furthermore, once you find the greatest common divisor m, find $k, \ell \in \mathbb{Z}$ such that $ka + \ell b = m$.

- $a = 234$ and $b = 165$.
- $a = 562$ and $b = 471$.

Interlude: We saw how fast the Euclidean Algorithm ran in class. However, it is not obvious why the algorithm terminates so quickly. In the next problem, we work to understand the theory behind the speed. Let $a, b \in \mathbb{N}$ with $b \neq 0$. Write $a = qb + r$ where $q, r \in \mathbb{N}$ and $0 \leq r < b$. Notice that after one step of the algorithm, the new second argument r may not be much smaller than the original second argument b. For example, if $a = 77$ and $b = 26$, then we have $q = 2$ and $r = 25$. However, it turns out that after *two* steps of the Euclidean Algorithm, the new second argument will be at most half the size of the original second argument. This is what we will prove in the next problem. From this fact, it follows that on input $(a, b) \in \mathbb{N}^2$, the algorithm terminates in at most $2 \log_2 b$ many steps.

Problem 3: Let $a, b \in \mathbb{N}$ with $b \neq 0$. In the first step of the algorithm, we write $a = qb + r$ where $q, r \in \mathbb{N}$ and $0 < r < b$ (we can assume that $r \neq 0$ because otherwise the algorithm stops at the next step). In the next step of the algorithm, we write $b = pr + s$ where $p, s \in \mathbb{N}$ and $0 \leq s < r$. Show that $s < \frac{b}{2}$.
Hint: You may find it useful to break the problem into cases based on how large r is.

Problem 4: Show that $\{n \in \mathbb{Z} : \gcd(n, n + 2) = 2\} = \{2n : n \in \mathbb{Z}\}$.

Problem 5: Let $a, b \in \mathbb{Z}$, and assume that at least one of a or b is nonzero. Let $d = \gcd(a, b)$. Since d is a common divisor of a and b, we can fix $k, \ell \in \mathbb{Z}$ with $a = kd$ and $b = \ell d$. Show that $\gcd(k, \ell) = 1$.

Problem 6: Let $a, b, c \in \mathbb{Z}$. Suppose that $a \mid c$, that $b \mid c$, and that $\gcd(a, b) = 1$. Using only the material through Section 3.2 (so without using the Fundamental Theorem of Arithmetic), show that $ab \mid c$.