Math 565, Problem Set 1: *due Wednesday, January 10*

1. Let $a, b, c \in \mathbb{Z}$. Use the definition of divisibility to directly prove the following properties of divisibility.

   i) If $a|b$ and $b|c$, then $a|c$.

   ii) If $a|b$ and $b|a$, then $a = \pm b$.

   iii) If $a|b$ and $a|c$, then $a|(b+c)$ and $a|(b-c)$.

2. Let a, b, c, n be integers. Prove that

   i) If $a|n$ and $b|n$ with $\gcd(a, b) = 1$, then $ab|n$.

   ii) If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

3. Let a and b be positive integers.

   i) Suppose that there are integers u and v satisfying $au + bv = 1$. Prove that $\gcd(a, b) = 1$.

   ii) Suppose that there are integers u and v satisfying $au + bv = 6$. Is it necessarily true that $\gcd(a, b) = 6$? If not, give a specific counterexample, and describe in general all of the possible values of $\gcd(a, b)$.

   iii) Suppose that (u_1, v_1) and (u_2, v_2) are two solutions in integers to the equation $au + bv = 1$. Prove that a divides $v_2 - v_1$ and that b divides $u_2 - u_1$.

   iv) More generally, let $g = \gcd(a, b)$ and let (u_0, v_0) be a solution in integers to $au + bv = g$. Prove that every other solution has the form $u = u_0 + kb/g$ and $v = v_0 - ka/g$ for some integer k.

4. Let $a_1, a_2, \ldots, a_k$ be integers with $\gcd(a_1, a_2, \ldots, a_k) = 1$, i.e., the largest positive integer dividing all of $a_1, \ldots, a_k$ is 1. Prove that the equation
$$a_1 u_1 + a_2 u_2 + \cdots + a_k u_k = 1$$
   has a solution in integers $u_1, u_2, \ldots, u_k$. [Hint: Repeatedly apply the extended Euclidean algorithm. You may find it easier to prove a more general statement in which $\gcd(a_1, \ldots, a_k)$ is allowed to be larger than 1.]