Math 150 Homework 3 Solutions

1. Let $m, n \in \mathbb{Z}$ not both 0. We defined the greatest common divisor of m and n as a positive integer d such that
   (a) $d|m$ and $d|n$,
   (b) if c is an integer such that $c|m$ and $c|n$ then $c|d$.
   Prove that the greatest common divisor is unique. That is if d and d' both satisfy the two conditions above, then $d = d'$.

   Since $d|m$ and $d|n$, we know $d|d'$. So $d' = kd$ for some $k \in \mathbb{Z}$. In fact, we know $k > 0$ because d and d' are both positive. Similarly, $d = ld'$ for some $l \in \mathbb{Z}^+$. Hence
   $$d = ld' = l(kd) = (lk)d.$$
   Since $d \neq 0$, this implies $lk = 1$. But $k, l \in \mathbb{Z}^+$, so the only possibility is $k = l = 1$. Hence $d = d'$.

2. In this exercise, you will prove that our definition of the greatest common divisor is equivalent to the one you learned in middle school. Let $m, n \in \mathbb{Z}$ not both 0.
   Suppose $d_1 > 0$ is the greatest common divisor of m and n according to our definition:
   (a) $d_1|m$ and $d_1|n$,
   (b) if c is an integer such that $c|m$ and $c|n$ then $c|d_1$.
   Let d_2 be the common divisor of m and n that is the largest number among the common divisors. That is we know
   (a) $d_2|m$ and $d_2|n$,
   (b) if c is an integer such that $c|m$ and $c|n$ then $c \leq d_2$.
   Show that $d_1 = d_2$.

   Since $d_1|m$ and $d_1|n$, we know $d_1 \leq d_2$. This also shows that $d_2 > 0$. Since $d_2|m$ and $d_2|n$, we also know $d_2|d_1$. So $d_1 = kd_2$ for some $k \in \mathbb{Z}$. Since d_1 and d_2 are both positive, $k > 0$. But k is an integer, so $k \geq 1$. Hence $d_1 \geq d_2$. The only way to have both $d_1 \leq d_2$ and $d_1 \geq d_2$ is to have $d_1 = d_2$.

3. Let $a, b \in \mathbb{Z}$ not both 0. Remember that we say a and b are relatively prime if $\gcd(a, b) = 1$. Prove that a and b are relatively prime if and only if there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

   Suppose a and b are relatively prime. Then $\gcd(a, b) = 1$ and by the Euclidean Algorithm (or Bezout's Identity), there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

   Conversely, suppose that $1 = ma + nb$ for some $m, n \in \mathbb{Z}$. We will show that 1 satisfies the definition of the gcd for a and b. First, 1 is obviously positive and $1|a$ and $1|b$. Second, suppose $c \in \mathbb{Z}$ is such that $c|a$ and $c|b$. Then $a = xc$ and $b = yc$ for some $x, y \in \mathbb{Z}$. Now
   $$1 = ma + nb = m(xc) + n(yc) = (mx + ny)c.$$
   Since $mx + ny$ is an integer, this shows $c|1$. This is true for any common divisor c of a and b, so 1 is actually a greatest common divisor. Therefore a and b are relatively prime.